Software Requirements Specification (SRS)
for
Configuration Management (CM) Services
of the
Defense Information Infrastructure (DII)
Common Operating Environment (COE)

Version 1.0 Final
25 January 1999
CM-170-900-01

This document is **UNCLASSIFIED** in its entirety

Prepared for and by:

Defense Information System Agency (DISA)
Joint Interoperability and Engineering Organization (JIEO)
Center for Integration (CFI)
Operational Support Facility (OSF) Location
Configuration Management Division (JEJE)
45335 Vintage Park Plaza
Sterling, Virginia 20166-6701

Software Requirements Specification (SRS) for Configuration Management (CM) Services of the Defense Information Infrastructure (DII) Common Operating Environment (COE)

Version 1.0 Final
25 January 1999
CM-170-900-01

Prepared for:

DISA/JEJE
ATTN: Ms. Jo Osborne Tate
45335 Vintage Park Plaza
Sterling, VA 20166-6701

Contract Number: DCA100-97-D-0043
Task Order Number: 0026, Task 3.2.1
CDRL Number: A048

Prepared by:

Science Applications International Corporation
8301 Greensboro Drive, Suite 940
McLean, VA 22102-3799

Booz·Allen & Hamilton, Inc.
8283 Greensboro Drive
McLean, VA 22102-3838

This page intentionally left blank.

Signature Sheet

The Software Requirements Specification (SRS) for Configuration Management (CM) Services of the Defense Information Infrastructure (DII) Common Operating Environment (COE), Final, 25 January 1999:

SUBMITTED BY:

_____

JO OSBORNE TATE, GS-15
Chair, Configuration Management Technical Working Group (CM TWG)

APPROVED BY:

_____

DAWN C. HARTLEY, SES-4
Chief Engineering Executive for Information Processing

NOTE: This document is maintained by the Configuration Management Technical Working Group (CM TWG). Comments concerning this document should be submitted electronically to the Chair, CM TWG, Jo Osborne Tate, at tate3j@ncr.disa.mil.

This page intentionally left blank.

Table of Contents

TABLES

FIGURES

SECTION 1. SCOPE

1.1 Identification

This Software Requirements Specification (SRS) describes the software requirements for the Configuration Management (CM) Services area of the Defense Information Infrastructure (DII) Common Operating Environment (COE). CM Services software is composed of applications and tools that support the accomplishment of CM functions associated with the four CM disciplines: Configuration Identification and Selection, Configuration Control, Configuration Status Accounting, and Configuration Audits. SRS requirements for automating support functions associated with the four CM disciplines address support for each product life cycle phase (pre-development, development, pre-production, and production). CM Services software requirements specified in this SRS are structured to encompass CM support services for the DII COE architecture as well as any system riding on the DII COE architecture. CM Services software requirements are identified, prioritized and tracked by the CM Technical Working Group (TWG) of the DII COE Architecture Oversight Group (AOG).

This document contains the total objective set of DII COE CM Services software requirements that DISA, as the Executive Agent (EA) of the DII COE, strives to fulfill. This document only applies to those CM support applications that fall under the direct control and supervision of the CM TWG.

1.2 System Overview

CM Services software is a collection of DII COE-compliant applications and tools used by DII COE management and engineering staff to execute the formal CM processes required for life cycle support of the DII COE and systems built on the DII COE. CM Services software functional requirements encompass all four CM disciplines throughout the four life cycle phases of DII COE products: Pre-Development, Development, Pre-Production and Production. Many of the services currently available in CM Services software are readily accessible to DII COE developers and users, such as support for registration of segments, submitting change requests, and requesting configuration status information.

A key component of the CM Services system is the Management Information System (MIS). The purpose of the MIS is to maintain a database of information for use in managing the pre-development, development, pre-production, and production of DII COE software and related documentation. The information collected in the MIS pertains to segments, individual problem reports written against those segments, and documents maintained in support of the segments. The ultimate goal of the MIS is a single, cradle-to-grave electronic management system for segments and related objects, i.e., documents, problem reports, changes, waivers, distributable code, etc.

CM Services software will also provide the capability to electronically receive and distribute electronic DII COE assets over the Internet and local networks with enhanced audit, security and performance capabilities. A developer will be able to electronically input the data pertaining to a segment and supporting objects before delivering it to the CFI. Once delivered, automated electronic acceptance and screening capabilities of CM Services software will determine whether the segments and supporting objects meet developer delivery requirements.

Upon delivery and acceptance, segment delivery data will be copied into the appropriate MIS table sets with minimal human labor. Once the data are available, authorized engineering and testing personnel can update it with the results of testing and query against it as necessary. The CM Services software will also provide facilities for internal distribution of delivered segments to other activities such as DII COE Engineering, Integration and Test. When the segment is deemed releasable, using Release Control Panel quality control indicators, the software release documentation can be generated automatically and the segment forwarded for electronic distribution.

The electronic receipt and distribution capability will be a key part of the "Just-in-Time" Delivery Schedule process for scheduling pre-production work based on delivery of final products. The "Just-in-Time" Delivery Schedule provides DII COE software CM, Engineering, Integration and Test planning schedules calculated based on planned software release dates and build list contents. The "Just-in-Time" Delivery Schedule will be used to assist DII COE CM, Engineering, Integration and Test personnel in scheduling and balancing workloads and to advise developers as to when major components of DII COE software must be finalized and delivered to avoid schedule impacts.

1.2.1 Configuration Management Architecture

The CM Architecture concept allocates functional areas of CM to the four CM disciplines: Configuration Identification and Selection, Configuration Control, Configuration Status Accounting, and Configuration Audits. In addition, the CM Architecture concept emphasizes the interrelationships between these CM functional areas and the applicability of certain functional areas to more than one discipline. For example, Commercial Off-The-Shelf (COTS) license planning and management functions span all four CM disciplines: COTS licensing requirements are identified for acquisition planning as part of Configuration Identification and Selection; management and distribution of acquired licenses is performed as part of Configuration Control; tracking the status of available and used licenses is part of the Data Tracking functional area of Configuration Status Accounting; and, auditing of license use and allocation is conducted as part of Configuration Audits.

The CM Architecture concept also captures the changes in functional areas allocated to each discipline as a project progresses through the four product life cycle phases: pre-development, development, pre-production, and production. For example, during the pre-development stage, Configuration Audit functional areas primarily consist of audit scheduling, agenda and facility planning, participant identification, and verifying contractor design solutions against requirement documentation baselines. The principal focus is on developing the Configuration Audit strategy. By the production phase, products have reached maturity, comprehensive sets of baseline documentation are established, and fielding of system hardware and software is initiated. Hence, during the production phase, audit functional areas expand to encompass:

- Verifying the integrity and accuracy of production hardware and software against baselined documentation and approved changes
- Checking documentation, software and hardware inventories
- Monitoring COTS licensing status, checking for violations, expiring licenses, and license allocation versus usage

- Verifying Web information is accurate and complete, and links to other sites are valid
- Conduct of physical and functional audits, and resolution of noted discrepancies and problems
- Revalidating risk assessments and adjusting risk mitigation strategies as needed;
- Preparing for Operational Test by reviewing and evaluating previous test results, safety, reliability, availability, maintainability, logistics support, CM support, security, and test resources.

A summary of the CM Architecture structure and component functional areas for each of the product life cycle phases is provided in the paragraphs that follow.

1.2.1.1 Pre-Development CM Architecture

CM functional areas during the pre-development life cycle phase focus on establishment and maintenance of CM guidelines and processes, establishing and controlling changes to the functional baseline baselines, establishing the CM MIS, and implementing secure access to MIS data for a Controlled Community of Interest. The specific CM functional areas that support pre-development processes are shown in Figure 1.2.1.1-1.

1.2.1.1.1 Configuration Identification and Selection

TBD

1.2.1.1.2 Configuration Control

TBD

1.2.1.1.3 Configuration Status Accounting

TBD

1.2.1.1.4 Configuration Audit

TBD

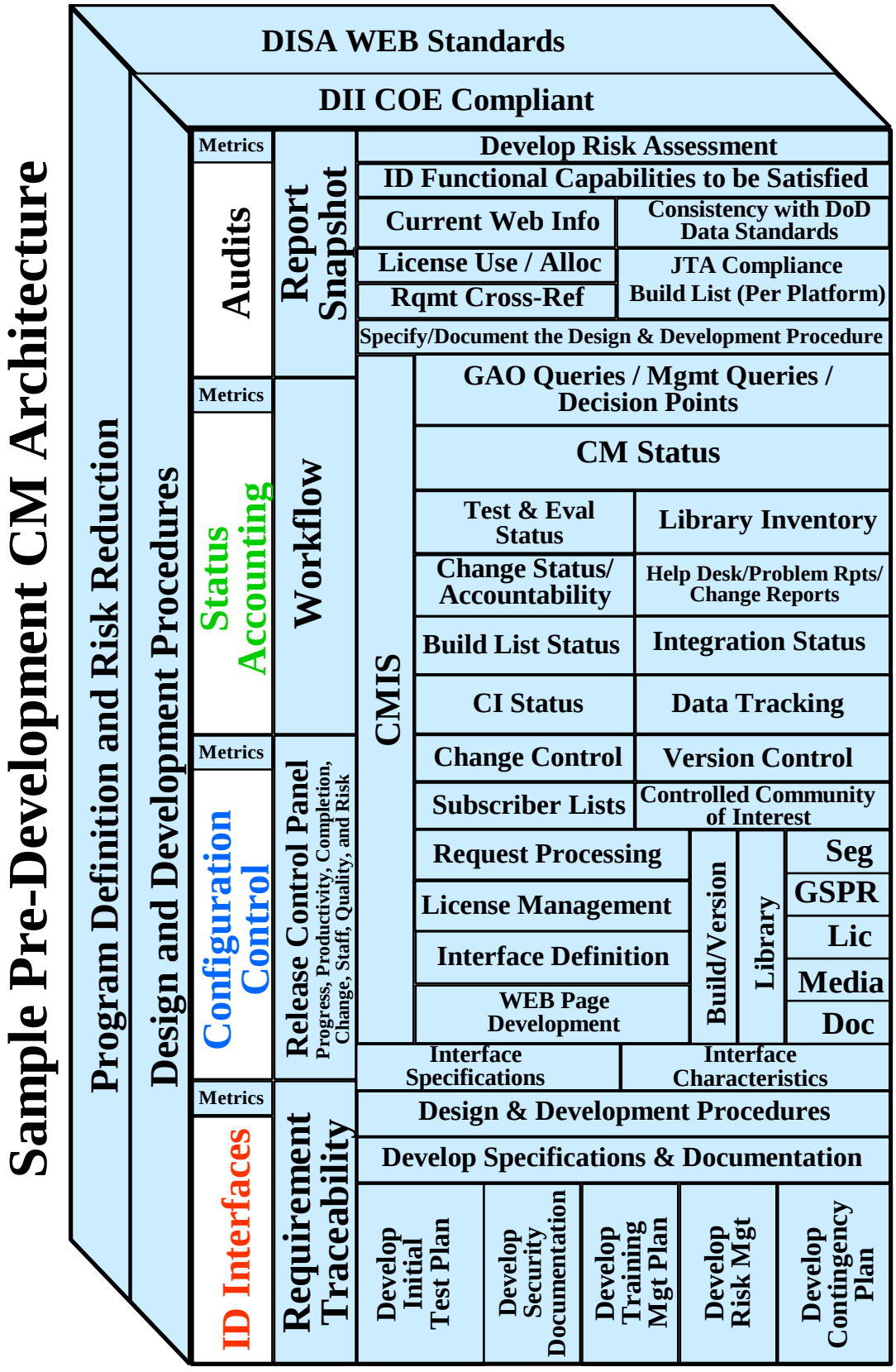

Figure 1.2.1.1-1. Pre-Development CM Architecture

1.2.1.2 Development CM Architecture

CM functional areas during the development life cycle phase focus on finalizing functional and allocated baselines, developing the production baseline, ensuring MIS data content (data elements and relationships) meets development and pre-production life-cycle phase data requirements and access to MIS data is controlled, and implementing software and documentation change control processes. The specific CM functional areas that support development phase processes are shown in Figure 1.2.1.2-1.

1.2.1.2.1 Configuration Identification and Selection

During the development phase, Configuration Identification and Selection functional areas support the implementation and maintenance of CM processes for identifying, selecting, and tracking CIs throughout their life-cycle. The specific functional areas supporting Configuration Identification and Selection during the development phase are summarized below.

- **Requirement Definition and Traceability** - During the development life-cycle phase, requirement traceability functions ensure all requirements have been mapped into baseline performance specifications and development test plans.
- **Configuration Management Planning** - Management planning activities to be supported during development include update of CM Plans and policy documentation to reflect process improvements, defining data requirements for pre-production life-cycle phase, and refining approaches for CM data collection and dissemination.
- **Configuration Item (CI) Identification** - CI identification functions assign identifiers to CIs including documentation, software, and hardware, and tracking identification of traceable items to contractor assigned identification and/or serial numbers.
- **Build Planning** - In the development phase, build planning functions support development, review, and update of proposed build plans, and track the status and priority of CIs contained in the proposed build plans.
- **License Planning** - License planning functions support collection, review and evaluation of information on COTS licenses needed to support proposed build plans.
- **Prefix/Segment/Socket Registration** - During the development phase, registration functions enable reservation of segment prefixes and sockets for segments under development.
- **Test Readiness Review** - Test Readiness Review functions during the development phase primarily focus on completion of test plans, including the testing schedule, facility(s), and resources required for testing support.
- **Schedule Calendar** - In the development phase, schedule calendar functions track scheduled completion dates for documentation and software CIs, design reviews, milestone decisions, and IPT, TWG and CCB action items.

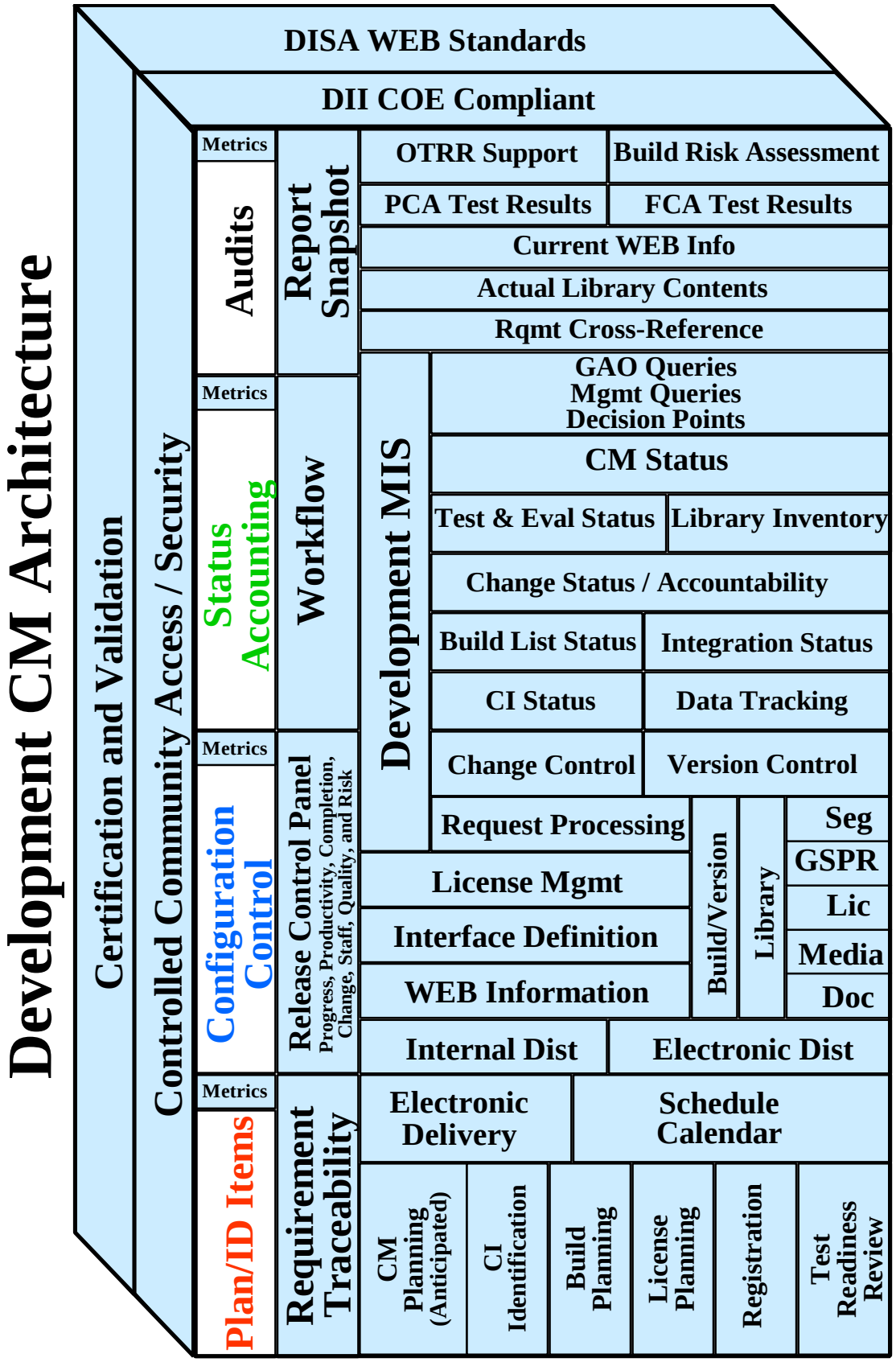

Figure 1.2.1.2-1. Development CM Architecture

- **Electronic Submission** - Electronic submission functions support the on-line, automated submission of baseline documentation by developers and organizations external to the CFI.
- **Electronic Acceptance** - Electronic acceptance functions support the on-line, automated verification and acceptance processes for receiving documentation electronically submitted by developers.
- **Metrics** - Configuration identification metrics during the development phase measure the traceability of requirements in baseline documentation and the productivity and efficiency of CM processes supporting configuration identification. Metrics also track completion of required/scheduled actions during this phase, including approval of top-level and lower-level CI performance specifications, establishing an allocated baseline for each CI, and establishing a product baseline (after CI performance verification and documentation/product consistency verification).

1.2.1.2.2 Configuration Control

During the development phase, Configuration Control functional areas support initiating, processing and tracking of changes to baseline configuration items and support Configuration Control Board (CCB) operating procedures for change evaluation and disposition. The specific functional areas supporting Configuration Control during the development phase are summarized below.

- **Release Control Panel** - During the development phase, the Release Control Panel functions support the management of scheduled tasks, inspection of development phase processes (focusing on adherence to CM guidelines), metrics data collection, and controlled release of approved documentation.
- **Scheduling** - Scheduling functions support Configuration Control processes for scheduling and tracking the status of documentation and engineering drawings as they are delivered, evaluated and approved/disapproved for functional and allocated baselines, as well as scheduling appropriate items for CCB review.
- **Electronic Distribution** - Electronic distribution functions during development provide automated capabilities for distribution of approved configuration documentation.
- **Internal Distribution** - Internal distribution functions provide automated capabilities for distribution of developed software and/or electronic reusable assets to contractor engineering, test and integration activities.
- **Web Information** - During the development life-cycle phase, Web-based functions provide automated capabilities for posting assets on the Web, submitting change requests, and performing pre-registration activities with appropriate access controls.
- **Interface Definition** - Interface definition functions during development identify and track internal and external interfaces and interface requirements for DII COE and mission applications.

- **Baseline Information** - Baseline information functions track the CIs belonging to the functional and allocated baselines for each build and version of software, provide information on CIs proposed for production baselines, and report on baseline information.
- **Controlled Library** - Controlled library functions support delivery and control of baseline documentation, and maintain and protect them from unauthorized access and changes.
- **License Management** - License Management functions track COTS licenses required for development, integration and test of software CIs proposed for production baselines, as well as maintain information, including type of license, expiration date, and acquisition vehicle for each COTS license required.
- **Request Processing** - During development, request processing functions support initiation and processing of requests for DII COE and mission application documentation assets that are not already available on the Web.
- **Change Control** - During development, change control functions support identification, coordination, evaluation and disposition of problem reports, change requests, ECPs, and Requests for Deviation.
- **Version Control** - Version control functions support management of version control numbers, tracking of document and segment supercession, and tracking of segment and document versions targeted for each software build. **XXX**
- **Metrics** - Configuration control metrics during the development phase measure the cycle time of problem reports and change requests and the efficiency of CM processes supporting segment development and test.

1.2.1.2.3 Configuration Status Accounting

During the development phase, Configuration Status Accounting functions maintain information on the as-designed and as-built configuration of CIs and CI components, as well as the status and history of changes. The specific functional areas supporting Configuration Control during the development life-cycle phase are summarized below.

- **Data Tracking and Recording** - During development, data tracking and recording functions compile and correlate configuration status data from functional and performance specifications, test plans/procedures/results, audits, change requests, etc., for product status assessments and user data requirements.
- **CI Status Monitoring** - CI status monitoring functions compare demonstrated functional and performance capabilities of software with documented requirements and identify and report on discrepancies.
- **Build List Status** - During development, build list status functions support querying, reporting on and controlling access to information on proposed software release build lists.
- **Configuration Change Status** - Development configuration change status functions support identifying and reporting on the status of problem reports and change requests and proposals being tracked by the MIS.

- **Change Accountability** - During development, change accountability functions support unique identification and traceability of every problem report and change request/proposal submitted, all the way to implementation.
- **Inventory of Libraries** - During development, library inventory functions track the contents of software, documentation, GSPR, and COTS license libraries and manage access to those libraries.
- **Status Accounting Information Access and Control** - Status accounting information access and control functions implement controlled access to baseline CI status information to "Controlled Communities of Interest".
- **Metrics** - Configuration status accounting metrics during the development phase track discrepancies between software requirements and demonstrated capabilities, and track the frequency of various types of change requests and problem reports.

1.2.1.2.4 Configuration Audit

During the development phase, Confi guration Audit functional areas support pre-audit planning and preparation. Support is also provided for verifying that all baseline documentation has been identified, completed and approved. The specific functional areas supporting Configuration Audit during the development phase are summarized below.

- **Documentation Library** - Documentation library functions track the applicable specifications, drawings, test documents, change requests/proposals, etc., associated with designated baselines being kept in the document library to support authorized user information needs and audits.
- **Software Library** - Software library functions, during the development phase, track software segment CIs being kept in the software library and support comparison of library contents to the license database for license compliance.
- **Current Web Information** - Current Web Information functions support comparison of assets currently available on designated web pages with assets and information associated with current approved baselines. Discrepancies, outdated assets, and invalid web links are identified and reported.
- **Functional Audit Test Report Results** - Functional Audit Test Report Results functions support tracking of issues, discrepancies, actions and minutes produced as a result of Functional Audits.
- **CI and System Requirement Cross-Reference** - Requirement Cross-Reference functions cross-reference CI and system requirements to the test procedures that validate the requirements.
- **Physical Audit Test Report Results** - Physical Audit Test Report Results functions support tracking of issues, discrepancies, actions and minutes produced as a result of Physical Audits.
- **Risk Assessment of Build** - Build Risk Assessment functions support impact analysis of software CI-associated events, processes, etc., with respect to the functional, compliance, security, and schedule aspects of planned software builds. These

functions also support development of risk mitigation strategies and risk assessment reports.

- **Test Readiness Review Support** - Test Readiness Review functions assist in identification of actions, documentation and software fixes required for conducting a successful Test Readiness Review.
- **Metrics** - Audit metrics functions support evaluation of audit processes by tracking audit scheduling, successful audit completions, and open action items and unresolved discrepancies.

1.2.1.3 Pre-Production CM Architecture

CM functional areas during the pre-production life cycle phase focus on finalizing production baselines, ensuring CM data maintained in the MIS is complete and accurate, and implementing secure access to MIS data and production items for a Controlled Community of Interest. The specific CM functional areas that support pre-production processes are shown in Figure 1.2.1.3-1.

1.2.1.3.1 Configuration Identification and Selection

During the pre-production phase, Configuration Identifi cation and Selection functional areas support processes for preparing and coordinating product acceptance and distribution mechanisms. Product line items are checked to ensure item identification numbers are assigned, performance and interfaces are clearly documented, all requirements are traceable, all approved changes have been incorporated, and product compliance, functional and integration testing has been successfully completed. The specific functional areas supporting Configuration Identification and Selection during the pre-production phase are summarized below.

- **Requirement Definition and Traceability** - In the pre-production phase, requirement traceability checks ensure all requirements have been mapped into computer program requirements, and that requirements can be traced to test procedures.
- **Configuration Management Planning** - Management planning activities during pre-production include update of CM Plans and policy documentation to reflect process improvements and ensuring the appropriate level of resources are in place for conducting CM.
- **Configuration Item (CI) Identification** - CI identification functions ensure items are appropriately identified and marked, and performance, interface and other attributes are clearly documented and are used as the basis for configuration control.
- **Build Planning** - In the pre-production phase, build planning functions support review, modification and querying/reporting on information in proposed and approved build plans, as well as maintaining historical records on previous plans.
- **License Planning** - License planning functions support review of information on COTS licenses required for each DII COE software release to support cost effective license acquisition.

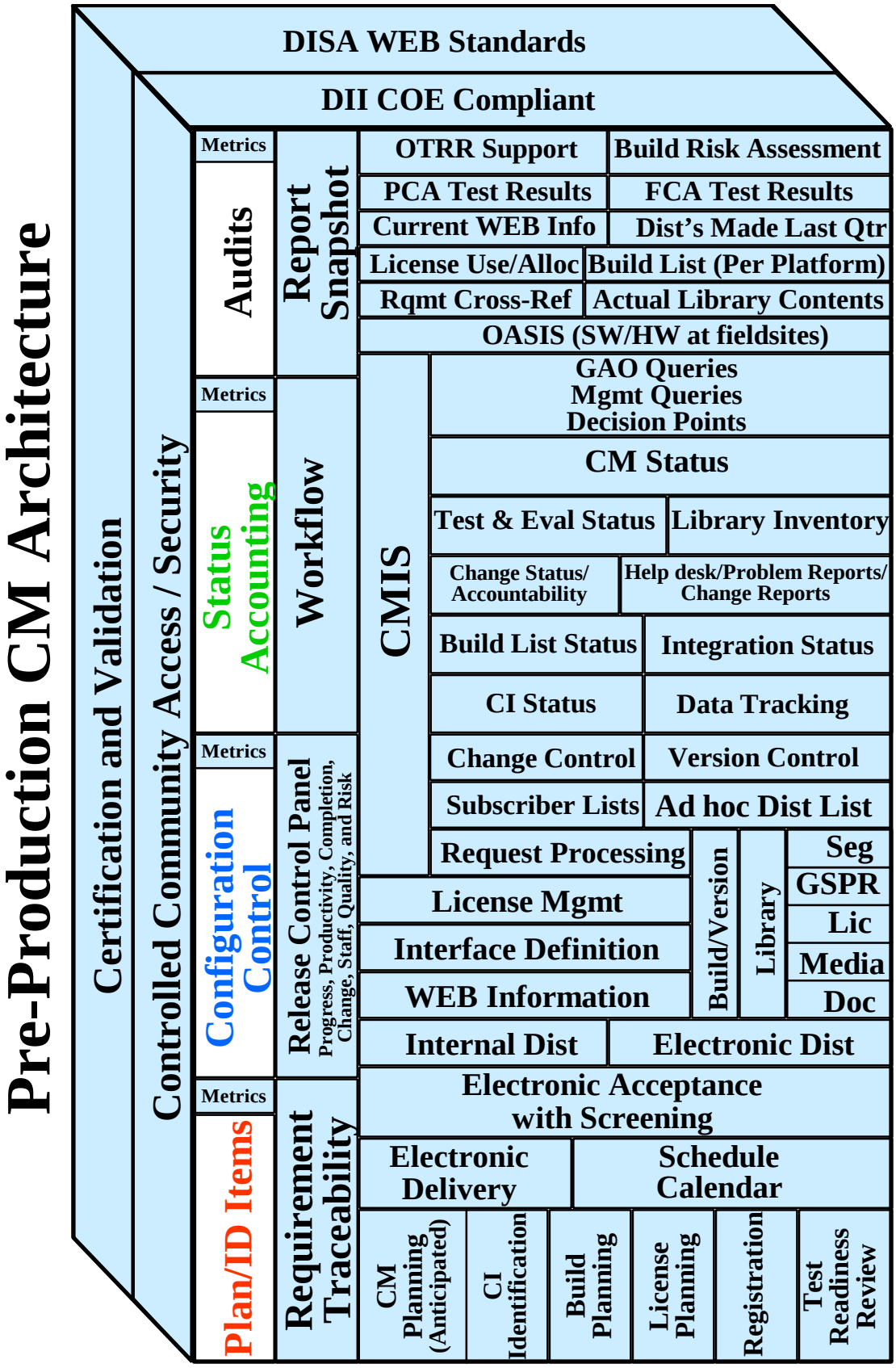

Figure 1.2.1.3-1. Pre-Production CM Architecture

- **Prefix/Segment/Socket Registration** - During the pre-production phase, registration functions support on-line registration of segment prefixes, segments and sockets. Registration information is then used to support CFI workload planning and to verify delivered products were pre-registered and are consistent with pre-registration information.
- **Test Readiness Review** - Test Readiness Review activities under configuration identification during the pre-production phase primarily focus on identifying the build to be used for Operational Testing (OT), and the testing schedule, facility(s), and resources required for testing support.
- **Schedule Calendar** - In the pre-production phase, schedule calendar functions support scheduling developer deliveries and balancing workloads for acceptance, test and integration of delivered software.
- **Electronic Submission** - Electronic submission functions support the on-line, automated submission of software and documentation by developers and organizations external to the CFI.
- **Electronic Acceptance** - Electronic acceptance functions support the on-line, automated verification and acceptance processes for receiving software and documentation electronically submitted by developers.
- **Metrics** - Configuration identification metrics during the pre-production phase measure the traceability of requirements in baseline documentation and the productivity and efficiency of CM processes supporting configuration identification.

1.2.1.3.2 Configuration Control

During the pre-production phase, Configuration Control functional areas support processes for initiating changes to established baselines and support Configuration Control Board (CCB) operating procedures for change evaluation and disposition. In addition, these functions support the initiation, review and approval/disapproval of Requests for Deviation from required documentation. The specific functional areas supporting Configuration Control during the pre-production phase are summarized below.

- **Release Control Panel** - During the pre-production phase, the Release Control Panel functions support the management of scheduled tasks and controlled release of approved software and documentation. Functions to measure progress, productivity, completion, change, staff, quality and risk provide management with the basis for making informed decisions.
- **Scheduling** - Scheduling functions support Configuration Control processes for scheduling and tracking the status of segments as they are delivered, accepted, integrated, tested and approved/disapproved for release.
- **Electronic Distribution** - Electronic distribution functions during pre-production provide automated capabilities for distribution of electronic reusable assets using the Internet with enhanced audit, security and performance capabilities.
- **Internal Distribution** - Internal distribution functions provide automated capabilities for distribution of electronic reusable assets within the CFI to engineering, test and integration activities.

- **Web Information** - During the pre-production phase, Web-based functions provide automated capabilities for posting assets on the Web, submitting change requests and requests for DII COE assets, and performing pre-registration activities with appropriate access controls.
- **Interface Definition** - Interface definition functions during pre-production maintain information on identified internal and external interfaces for DII COE and mission applications, including interface agreements and decisions and actions of Interface Control Working Groups (ICWGs).
- **Baseline Information** - Baseline information functions track the CIs belonging to baselines for each build and version of software and report on DII COE and mission application baselined information.
- **Controlled Library** - Controlled library functions support delivery and control of baseline documentation and software, and maintain and protect them from unauthorized access and changes.
- **License Management** - License Management functions automate single point license management and provide access to COTS license information. [Note: Although DISA does not plan to buy or distribute COTS licenses, Service/Agency tool requirements for managing acquired licenses are within the scope of this document. The DISA CFI expects DII COE customers to provide proof of required licenses before downloading software.]
- **Request Processing** - During pre-production, request processing functions support initiation and processing of requests for DII COE and mission application software and documentation assets that are not already available on the Web.
- **Subscriber Lists** - Subscriber list functions track DII COE subscriber information to support distribution of DII COE assets and determine customer licensing requirements.
- **Ad hoc Distribution Lists** - Ad hoc distribution list functions track information on DII COE subscribers that receive assets on an infrequent basis.
- **Change Control** - During pre-production, change control functions continue to support identification, coordination, evaluation and disposition of problem reports, change requests, ECPs, and Requests for Deviation.
- **Version Control** - Version control functions continue to support management of version control numbers, tracking of segment supercession, and tracking of segment and document versions associated with each software build
- **Metrics** - Configuration control metrics during the pre-production phase measure the cycle time of problem reports and change requests, the number of requests for DII COE assets, and the efficiency of CM processes supporting segment engineering, integration and test.

1.2.1.3.3 Configuration Status Accounting

During the pre-production phase, Configuration Status Accounting functions maintain information on the as-designed, as-built, as-delivered, or as-modified configuration of CIs and CI

components, as well as the status and history of changes. The specific functional areas supporting Configuration Control during the pre-production phase are summarized below.

- **Data Tracking and Recording** - During pre-production, data tracking and recording functions compile and correlate configuration status data from performance specifications, test plans/procedures/results, audits, change requests, etc., for product status assessments and user data requirements.
- **CI and System Status Monitoring** - CI and system status monitoring functions compare software performance with documented thresholds and identify and report on threshold violations.
- **Build List Status** - During pre-production, build list status functions support querying, reporting on and controlling access to build information.
- **Configuration Change Status** - Pre-production configuration change status functions support identifying and reporting on the status of problem reports and change requests and proposals being tracked by the MIS.
- **Change Accountability** - During pre-production, change accountability functions continue to support unique identification and traceability of every problem report and change request/proposal submitted, all the way to implementation.
- **Inventory of Libraries** - During pre-production, library inventory functions track the contents of software, documentation, GSPR, and COTS license libraries and manage access to those libraries.
- **Status Accounting Information Access and Control** - Status accounting information access and control functions implement controlled access to baseline CI status information to "Controlled Communities of Interest".
- **Metrics** - Configuration status accounting metrics during the pre-production phase measure threshold violations compared to actual performance parameters of software, track the frequency of various types of change requests and problem reports, and in general, identify potential problem areas for which additional resources may be required.

1.2.1.3.4 Configuration Audit

During the pre-production phase, Configuration Audit functional areas support pre-audit planning and preparation. Support is also provided for verifying configurations and documentation are consistent with operational and support requirements, and that all baseline documentation has been identified and approved. The specific functional areas supporting Configuration Audit during the pre-production phase are summarized below.

- **OASIS (Software/Hardware at Fieldsites)** - During the pre-production phase, system inventory support functions track fielded hardware and software, compare as-built with as-designed baseline specifications, and assist in the conduct of physical audits.
- **Documentation Library** - Documentation library functions track the applicable specifications, drawings, test documents, change requests/proposals, etc., associated

with designated baselines that are being kept in the document library to support authorized user information needs and audits.

- **Software Library** - Software library functions, during the pre-production phase, track software segment CIs being kept in the software library and support comparison of library contents to appropriate baselines and the license database for license compliance.
- **Build List (Per Platform)** - During pre-production, build list (per platform) functions compare the as-built CI configuration of individual platforms to the appropriate approved build list and report on identified discrepancies.
- **Fielded Equipment** - During pre-production, functions associated with fielded equipment support identification of fielded models, firmware revision level, and tracking of problem reports related to hardware platform models and their firmware.
- **License Use/Allocation** - License use/allocation functions compare the number of licenses allocated versus the number of licenses used, and identify associated licensing agreements, violations, and expirations.
- **Distributions Made Last Quarter** - Functions supporting Distributions Made Last Quarter track information and compile statistics on how, how many, when and where assets were distributed during the past quarter to support audit and asset management planning.
- **Current Web Information** - Current Web Information functions support comparison of assets currently available on designated web pages with assets and information associated with current approved baselines. Discrepancies, outdated assets, and invalid web links are identified and reported.
- **Functional Audit Test Report Results** - Functional Audit Test Report Results functions support tracking of issues, discrepancies, actions and minutes produced as a result of Functional Audits.
- **CI and System Requirement Cross-Reference** - Requirement Cross-Reference functions cross-reference CI and system requirements to the test procedures that validate the requirements.
- **Physical Audit Test Report Results** - Physical Audit Test Report Results functions support tracking of issues, discrepancies, actions and minutes produced as a result of Physical Audits.
- **Risk Assessment of Build** - Build Risk Assessment functions support impact analysis of events, processes, etc., with respect to the functional, compliance, security, and schedule aspects of planned software builds. These functions also support development of risk mitigation strategies and risk assessment reports.
- **Test Readiness Review Support** - Test Readiness Review functions assist in identification of actions, documentation and software fixes required for conducting a successful Test Readiness Review.
- **Metrics** - Audit metrics functions support evaluation of audit processes by tracking audit scheduling, successful audit completions, and open action items and unresolved discrepancies.

1.2.1.4 Production CM Architecture

During the production life-cycle phase, production software and documentation is approved, released and baselined for change control by the appropriate Configuration Control Authority. CM functional areas during the production life cycle phase focus on production baseline distribution and verification as well as collecting and providing access to operation and maintenance information for the current configuration. Feedback is collected from product users for planning product refinements. The specific CM functional areas that support production processes are shown in Figure 1.2.1.4-1.

1.2.1.4.1 Configuration Identification and Selection

During the production phase, Configuration Identification and Selection functions establish and maintain the production baseline. Individual items required for logistics support and designated for separate procurement are identified and tracked as additional configuration items (CIs) associated with the product baseline. Most identification and selection functions remain basically unchanged from the pre-production to the production phase. A few differences worth noting are summarized below.

- **Configuration Management Planning** - CM planning activities during production include update of CM plans and policy documentation to reflect process improvements, new deployment information, changes in support/maintenance planning, and planning for end of production, demilitarization and disposal.
- **Build Planning** - In the production phase, build planning functions support querying and reporting on information in approved build plans, as well as maintaining historical records on previous plans.
- **Schedule Calendar** - In the production phase, schedule calendar functions support coordination of deployment strategies, training, logistics support, and licensing requirements with scheduled software releases.
- **Metrics** - Configuration identification metrics during the production phase measure events such as engineering change approval rate and cycle time, number of configuration audits planned, held and successfully completed (all actions), and the number of deviation requests and waivers, including the percent of recurring deviation requests and waivers.

1.2.1.4.2 Configuration Control

During the production phase, Configuration Control functions continue to support processes for initiation, review and approval/disapproval of changes to established baselines. For the most part, production phase configuration control functions are basically the same as during the pre-production phase. The configuration documentation associated with each CI provides the basis for configuration control, logistics support, post-deployment software support, and re-procurement. One minor difference is that functions to support segment registration, electronic

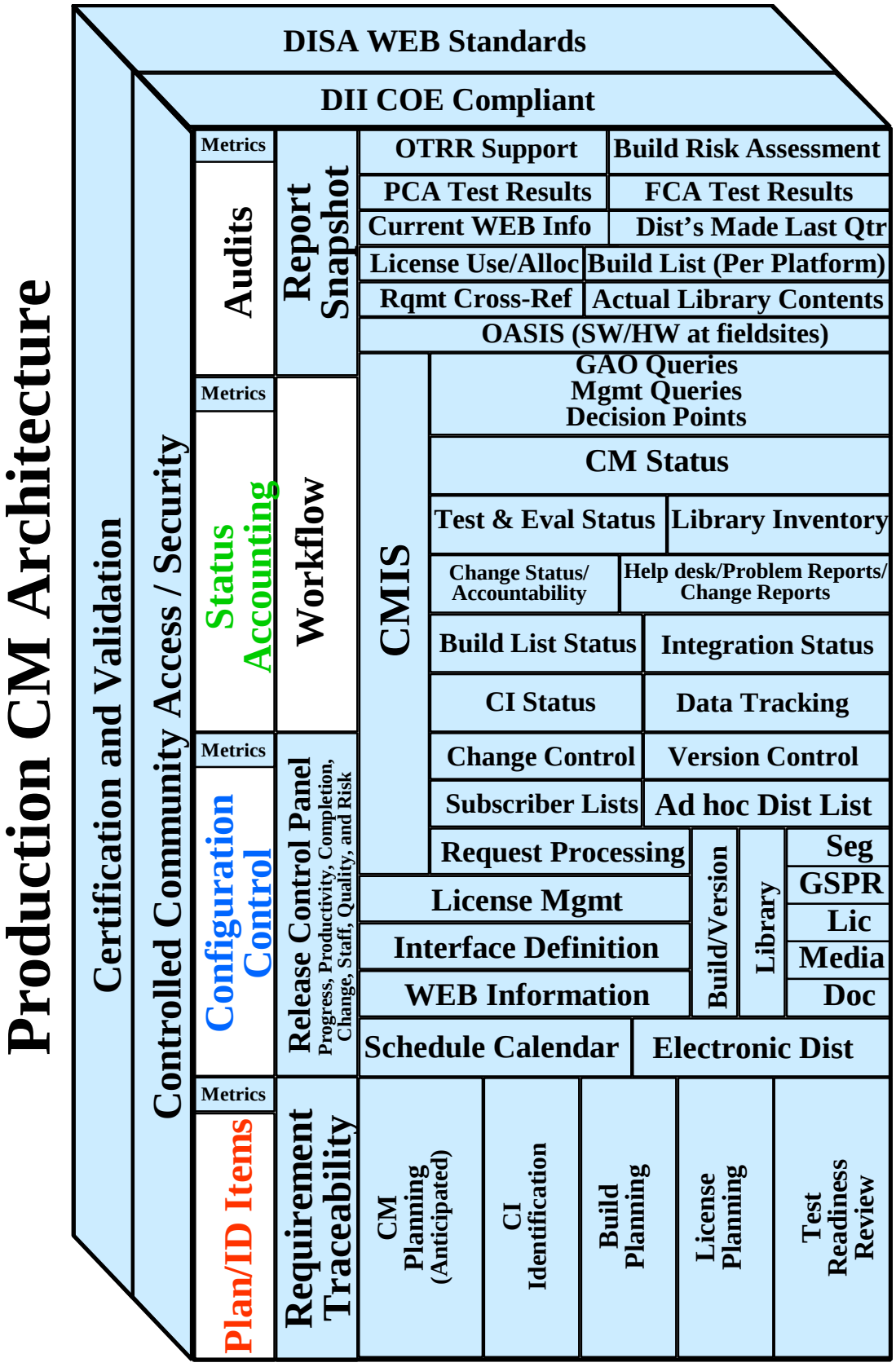

Figure 1.2.1.4-1. Production CM Architecture

delivery of segments to the integration facility, and electronic acceptance/screening of segments are no longer needed during the production life-cycle phase.

1.2.1.4.3 Configuration Status Accounting

During the production phase, Configuration Status Accounting function s continue to maintain information on the configuration of CIs and the status and history of changes. Correct, timely configuration information facilitates decision making on changes, deployment of assets, determining appropriate replacements, and performing updates/upgrades. Most status accounting functions remain basically unchanged from the pre-production to the production phase. A few differences worth noting are summarized below.

- **Build List Status** - During production, build list status functions track the build lists for installed platforms.
- **Configuration Change Status** - During the production life-cycle phase, configuration change status functions continue to report on the status of problem reports and change requests being tracked by the MIS. In addition, configuration change status functions report on the effectivity and installation status of configuration changes to all CIs, including those changes resulting from retrofit and by replacement through maintenance action.

1.2.1.4.4 Configuration Audit

Production phase Configuration Audit functions continue to provide the audit planning and preparation support described for the pre-production phase as well as supporting conduct of on site FCAs and PCAs. Configuration Audit support functions remain basically unchanged from the pre-production to the production phase. One minor difference is that Build Risk Assessment functions also support revalidating risk assessments and adjusting risk mitigation strategies as needed.

1.2.2 DII COE Configuration Structure

Segments that comprise DII COE and systems based on DII COE are categorized as belonging to one of four areas of the DII COE Configuration Structure: the DII COE Kernel, Infrastructure Services, Common Support Applications, or Software Development Services (i.e., toolkits). The DII COE Kernel is the minimal set of software required on every DII COE-based platform regardless of how the platform will be used. The DII COE Kernel includes the Operating System, Windowing Services, and Security Management Services. Infrastructure Services provide the framework for *exchanging* data and Common Support Applications provide the framework for *sharing* data. Infrastructure Services provide low level tools for managing and distributing the flow of data throughout the system. Common Support Applications provide the architectural framework for managing and disseminating information flow throughout the system. This level contains facilities for processing and displaying common data formats and for information integration and visualization. The Software Development Services consist of a collection of toolkits to assist the developer in creating mission application software. The toolkits are required only during software development, not during runtime at an operational site.

The CM Services area of DII COE is part of DII COE Common Support Applications, as shown in Figure 1.2.2-1. Configuration Management Services software runs on top of the DII

COE and provides the infrastructure necessary for receiving, processing and distributing CM data both internally within the CFI and externally with DII COE user organizations.

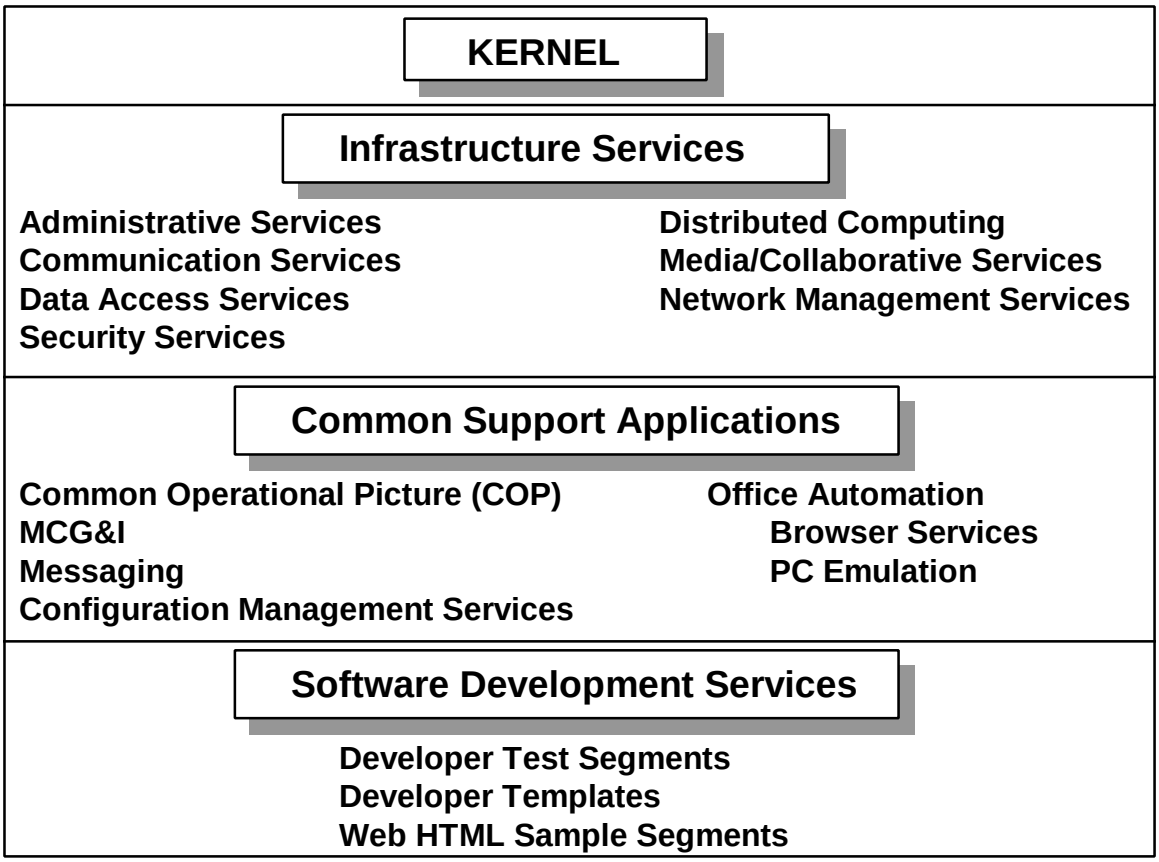

Figure 1.2.2-1. DII COE v3.3 Configuration Structure

1.2.3 Architecture Versus System

The DII COE is a "plug and play" open architecture designed around a client/server model. The key to this "plug and play" concept is conformance to the DII COE through adherence to software development guidance provided in the current version of the *DII Common Operating Environment Integration and Runtime Specifications*, the *DII Common Operating Environment Software Quality Compliance Plan*, and the *Joint Technical Architecture (JTA)*.

The DII COE is *not* a system; it is a *foundation* for building an open system. Functionality is easily added to or removed from the target system in small manageable units called *segments* (a collection of one or more software modules managed as a unit that provides specialized software functionality). The DII COE concept emphasizes both software reuse and interoperability and encompasses the following:

- An architecture and approach for building interoperable systems
- An environment for sharing data between applications and systems
- An infrastructure for supporting mission-area applications
- A rigorous definition of the runtime execution environment

- A reference implementation on which systems can be built
- A collection of reusable software components and data
- A rigorous set of requirements for achieving DII COE compliance
- A set of guidelines, standards, and specifications that describe how to reuse existing software and how to properly build new software so that integration is seamless and, to a large extent, automated.

The DII COE architecture is fully compliant with the *Department of Defense (DoD) Technical Architecture for Information Management (TAFIM), Volume 3*. The DII COE, including the CM Services area of DII COE Common Support Applications, will evolve as necessary to maintain compliance with the JTA as per Mr. Emmett Paige's (Assistant Secretary of Defense) 23 May 1997 memo, *Implementation of Defense Information Infrastructure Common Operating Environment Compliance*. The JTA stipulates DII compliance as part of its requirements and replaces the standards guidance in the TAFIM as per an Office of the Secretary of Defense (OSD) directive dated 30 August 1996.

DISA is the technical integrator of the DII COE. As integrator, the DISA Joint Interoperability and Engineering Organization (JIEO) manages development and preparation of the DII COE to meet infrastructure requirements of a wide variety of users across the Department of Defense (DoD). The need for a well-structured and integrated CM process is recognized as a priority in the DoD communities using the DII COE. Because many DoD organizations are involved with evolving components of the DII COE and because the DII COE is not a system, but an infrastructure that is tailored to meet specific mission requirements, traditional CM support requirements need to be extended and tailored to address CM for the DII COE.

1.2.4 DII COE Configuration Management (CM)

The DII COE is currently fielded in systems throughout the DoD. Two such systems are the Global Command and Control System (GCCS) and the Global Combat Support System (GCSS). Both systems use the same DII COE infrastructure and integration approach and they use the same DII COE components for functions that are common. DII COE development is a process of continually evolving a stable baseline to take advantage of new technologies as they mature and to introduce new capabilities. But the changes are done one step at a time so that the warfighters always have a stable baseline product while changes between successive releases are perceived as slight. The CM structure for the DII COE provides the Services and Intelligence Community, who are building subscriber systems based on the DII COE, a formal voice in its evolution and insight into its plans and schedules.

To execute the CM functions for the DII COE and systems built on the DII COE, various tools and applications have been implemented by DII COE management and engineering staff. These tools form the initial core of the CM Services software. As DII COE development processes evolve, established CM processes may require periodic modification to capture emerging and changing CM policy and procedure requirements to support new DII COE and DII COE Command, Control, Communications, Computers, and Intelligence (C4I) system manufacturing and production processes. As new policies and process improvements are identified and approved, CM Services software will evolve to support new CM automated tool requirements and integrate DII COE CM processes throughout the DoD. Oversight, management, acquisition and development of CM Services software is the responsibility of the

CFI CM Division and the CM Technical Working Group (TWG). The purpose of the CM TWG is to identify, prioritize, and track DoD and other agency requirements and to coordinate implementation of CM for planning, control, status, and audits of DII COE and DII COE-compliant assets.

The CM TWG will provide the end-user community (i.e., authorized Service and Agency Points-of-Contact) with access to DII COE-compliant CM applications. The applications are broken into two broad categories. The first are those applications that are run out of the DISA DII COE management center. This category of applications would be installed on DII COE-compliant workstations or servers that function primarily as management workstations. The other category of applications are those components that run on end-user workstations, application servers, data servers, and so forth that remotely gather management information. This category of applications can be considered monitoring or reporting agents to the higher level management center. Combining these two categories of CM Services applications will give the designer of a DII COE-compliant system the tools necessary to effectively perform CM of their system.

The goal of the CM TWG is to create a library of segmented applications that can be used to perform all DII COE CM functions and management services. The library will consist mostly of COTS management software. However, some management applications will be government-of-the-shelf (GOTS) because they will provide specialized management functionality unique to DII COE CM. It is envisioned that all COTS CM Services applications will fall under the control and supervision of the CM TWG and be considered integral components of the DII COE.

The functional requirements identified for CM services are specified in Section 3. The requirements are divided among the four CM disciplines: Configuration Identification and Selection, Configuration Control, Configuration Status Accounting, and Configuration Audits. The paragraphs that follow provide a brief overview of the four CM disciplines, the associated CM functions, and how CM Services software is being implemented to support these functions .

1.2.4.1 Configuration Identification and Selection

Configuration Identification functions incrementally establish and maintain the definitive current basis for control and status accounting of a system and its configuration items (CIs) throughout their life cycle (pre-development, development, pre-production, and production, until de-militarization and disposal). During the pre-development phase, configuration identification activities focus on developing and implementing a method for categorizing and uniquely identifying the CIs to be managed. Interface agreements are established with associated Government programs/commands, as applicable. In addition, requirements traceability is established from top level to allocated requirement definitions and top level CI performance specifications. During the development phase, each system CI, including hardware, software, firmware, telecommunication, documentation and system change request/proposal CIs, is assigned a name and an alphanumeric identifier that uniquely identify the CI. These activities provide the foundation for all of the other Government CM functional activities. Also, during the development phase, an allocated baseline is established for each CI with the approval of top level and lower level CI performance specifications and traceability of requirements extends to test procedures. During the pre-production phase, a product baseline is established and configuration identification processes manage documentation, hardware and software created or revised as a result of approved engineering changes. In the production phase, established baselines are maintained and updated as system improvements and fixes are approved and implemented.

Through contractors, Integrated Product Te ams (IPTs) and other means, Configuration Identification provides approved configuration documentation to document the physical and functional characteristics of the system/item, establishes baselines for Government and contractor configuration control, creates records in the status accounting database, and provides documentation for configuration verification and audit. The continuous integrity of configuration identification is assured by good configuration control procedures.

1.2.4.1.1 Requirement Definition and Traceability

When viewed on a system basis, care must be exercised to assure that all of the top level requirements are accounted for in individual lower level documents. This is a key function of reviews such as system, preliminary and critical design reviews, but is greatly facilitated by the use of automated requirements allocation and traceability tools. Requirement definition and traceability functions provided by CM Services software shall implement policies and procedures controlling DII COE software requirements. These functions verify that DII COE product items and configurations meet source requirements and ensure DII COE requirements are traceable. These functions support:

- Management of requirements specifications for all DII COE segments and DII COE-compliant mission applications
- Management of requirements collected from Data Calls
- Modification of requirements for clarification and to add detail
- Development and implementation of processes to manage DII COE and mission application requirements traceability
- Establishing traceability of requirements from functional requirements specifications through development and testing documentation
- Validation of requirements traceability with test results.

1.2.4.1.2 Management Planning

Management planni ng is key to effective implementation of CM. CM Services software shall provide automated management planning functions to support:

- Product planning
- Identification of CI data to be recorded and tracked
- Establishment of processes for handling system requirements analysis, development, integration, testing, change implementation, performance measurement, and production of software
- Establishment of formal management structures to manage the processes and allocate the required resources.

Another aspect of configuration identification, to be considered during the pre-development and development phases, is interface management. All of the interfaces between co-functioning items need to be identified and documented as part of the planning process so that their integrity may be maintained through a disciplined configuration control process. For DII COE and systems based on DII COE, the Interface Control Working Group (ICWG) has been established as a formal interface management process to define and document interfaces. CM

Services software shall provide support for identifying, tracking and maintaining a status on newly proposed interfaces and interface agreements to support the information requirements of the ICWG and DISA engineering staff and to maintain the approval/disapproval status of proposed interfaces.

1.2.4.1.3 Configuration Item (CI) Identification

CM Services software shall provide automated CI identification support capabilities to include:

- Implementing approved CI identification methods
- Maintaining a defined documentation identification and release process
- Identifying the DII COE or mission application hardware and software CIs
- Identifying which processes of each CI need to be tracked and managed
- Tracking and management of each CI.

1.2.4.1.4 Build Plan Support

CM Services software shall provide automated Build Plan support functions for:

- Build Plan development and implementation processes required for DII COE and mission application development, testing and production
- Establishing management structures for managing Build Plan processes
- Developing the Build Plan with inputs from associated organizations
- Submitting the Build Plan to the approval organization.

1.2.4.1.5 License Planning

CM Services software shall provide automated functions for tracking, maintaining and reporting on COTS license information, including licensing agreements established between Services/Agencies. Automated support shall also be provided for maintaining customer profile information and for identifying license expirations and violations.

1.2.4.1.6 Segment Prefix/Segment/Socket/UID-GID Registration

CM Services software shall provide automated functions for segment prefix/segment/socket/User Identification (UID)-GID registration support, including:

- On-line registration of segment prefixes, segments, segment-unique Transmission Control Protocol/Internet Protocol (TCP/IP) sockets, segment-unique UIDs/GIDs
- Capturing segment information from segment registrants for storage in a catalog set of databases
- Maintaining, querying, and reporting on segment information collected from the DoD community.

1.2.4.1.7 Test Readiness Review

CM Services software shall provide automated functions for test readiness review support, including:

- Identification of segments/applications with poor performance records
- Identification of unresolved discrepancies
- Identification of actions required with respect to documentation deficiencies and resolving software issues, such as compliance, security and functionality
- Identification of key program milestone events and associated risks.

1.2.4.1.8 Inventory Support

CM Services software shall provide automated functions to support DII COE inventory activities. Support shall be provided for identifying, tracking and reporting system software, hardware and firmware CI information for defined system configurations and for individual sites.

1.2.4.1.9 Schedule Calendar

CM Services software shall provide automated scheduling functions to support:

- Identifying the DII COE and mission application development, testing, and production processes that require scheduling
- Deconflicting schedules, as required
- Reevaluating resource allocations based on established schedules and modifying schedules as required.

1.2.4.1.10 Electronic Submission

CM Services software shall provide automated capabilities for electronic submissions of DII COE software and documentation. When electronic submission is in place, the intent is for all submissions to be performed by the cognizant Service or Agency.

A key management planning tool for coordinating DII COE electronic and manual submissions is the CFI CM Division's web-based Delivery and Scheduling System. Electronic submission capabilities shall include automated support for incorporating submitted information into the MIS.

1.2.4.1.11 Electronic Acceptance

CM Services software shall provide automated capabilities for acceptance of developer software and documentation. Automated electronic acceptance support shall be provided for:

- Ensuring developer submissions meet software and documentation delivery requirements
- Verifying segments and segment information are consistent with information provided during segment/prefix pre-registration activities
- Verifying incorporation of approved fixes to problems reported
- Identifying associated waivers (and/or deviation requests)
- Identifying licensing requirements

- Identifying discrepancies.

1.2.4.1.12 Configuration Identification and Selection Metrics

Requirements for the implementation of metrics are incorporated into this SRS to support quantitative measurement of CM processes and DII COE product quality. The metrics, if properly applied, can give management important insight into the health and efficiency of Government and contractor DII COE CM processes and a basis for making informed decisions on software management issues. The metrics identified in this SRS focus on measuring internal CFI CM Division work processes, performance against customer requirements for maintaining and upgrading DII COE, performance of contractors, and adherence to planned budgets. Appendix B provides an overview of the metrics specified in this document and suggestions for their implementation.

The CM Services software metrics designed to measure configuration identification processes shall provide automated functions to support:

- Identification of potential DII COE and mission application problem scenarios
- Identification of metrics applicable to problem scenarios with which to classify, verify and validate the problems
- Development of processes with which to capture, maintain, analyze and report on DII COE and mission application problems
- Development of processes to alleviate the problems
- Development of processes with which to evaluate the success of the processes designed to alleviate the problems
- Incorporation of Project Control Panel gauges for assessing the general health of DII COE and DII COE-based system programs. When gauges are not in acceptable ranges, they indicate potential trouble to management. (See Appendix B for an overview of Project Control Panel gauges.)

Configuration identification metrics shall specifically capture metrics information on:

- Segment submissions
- Build plan functional capabilities
- Computer Software Configuration Item (CSCI) attributes
- COTS licenses
- Requirements traceability and changes.

1.2.4.2 Configuration Control

Configuration Control functions provide proper change control of system CIs during system development and evolution, and implement access controls to system and CI information. Configuration Control mechanisms receive input from Configuration Identification defining the current configuration baseline, and receive and process requests for engineering changes and modifications to fielded items. Configuration Control is also supported by information obtained from the Configuration Status Accounting (CSA) database as needed. The CSA information includes the current implementation status of approved changes and other pertinent information

concerning the configuration of items in design, in production and in the operational inventory. Configuration control provides input to status accounting about change identifiers, about the progress of change documentation through the steps in the configuration control decision/authorization process, and about the implementation status of authorized changes. Configuration Control functions also provide support for management of COTS licenses.

The configuration control process evolves from a less formal process in the pre-development phase of a program to a very disciplined and formal process during the development, pre-production and production phases. During the pre-development phase, configuration control processes are established and implemented for tracking the identification, review, coordination and status of changes to evolving system level specifications. During the development phase, established configuration control processes support change initiation, evaluation and disposition. Configuration controls manage implementation of approved Engineering Change Proposal (ECP) changes into configuration documentation defining performance, physical and functional characteristics and configuration of the products, as well as into CIs, and all affected products and services. During the pre-production phase, release controls measure progress, productivity, completion, change, staffing, quality and risk. Configuration control processes continue to support change initiation and CCB operating procedures for change evaluation and disposition. In addition support for processing, approving and tracking deviation requests and waivers from contractors is provided. During the production phase, version control and change control processes continue, and consistency of products, documentation, and resources for maintenance and training is validated for implemented changes.

1.2.4.2.1 Release Control Panel

CM Services software shall provide automated capabilities for implementing and evaluating DII COE software release controls, including:

- Maintenance of Release Milestone Schedules
- Providing reports on the progress and completion of scheduled tasks for assessing productivity
- Providing budget and cost tracking capabilities
- Reviewing and assessing staff requirements to meet anticipated workloads
- Providing the status and overall quality of all assets associated with a planned release
- Identifying and quantifying risks associated with pre-production efforts
- Identifying DII COE user organizations and maintenance of DII COE customer information.

1.2.4.2.2 Scheduling

CM Services software shall provide automated functions to support scheduling, i ncluding:

- Update of DII COE and mission application development, testing, and production schedules
- Deconfliction of schedules as required
- Reevaluating resource allocations using updated schedules and modifying them as required.

1.2.4.2.3 DII Asset Distribution (DAD)

CM Services software shall provide automated capabilities for distribution of electronic reusable assets using the Internet with enhanced audit, security and performance capabilities. The DII Asset Distribution (DAD) capability will be implemented as a distributed architecture, functioning on and through existing DoD networks including Secret Internet Protocol Routing Network (SIPRNET), Unclassified (but Sensitive) Internet Protocol Routing Network (NIPRNET) and Joint Worldwide Intelligence Communications System (JWICS) (Top Secret). DAD will be an infrastructure of multiple system and tool implementations adhering to the DAD architecture. DAD will also be a mission application, residing on the DII COE.

DAD assets include DII COE segments, software patches, database segments, and related tools, documentation and guidance information. Automated capabilities for supporting DII electronic asset distribution shall include:

- Ability for authorized users to browse assets, search for assets, select and download assets,
- Enabling authorized users to subscribe for notification of new or changed assets and to future download of new assets
- Distributing new assets automatically to users on designated subscription lists
- Electronic distribution of assets over SIPRNET (Secret), NIPRNET (Unclassified but Sensitive) and JWICS (Top Secret)
- Packaging assets selected by users into a single download that can be directed to any machine
- Creating, managing, modifying, and deleting DAD user groups
- Installing assets remotely on workstations or servers
- Managing links and interfaces between DAD libraries and instances
- Reporting on asset extraction accounts.

DAD will be used by and within United States DoD Services and Agencies and any other authorized organizations. DAD users will include defense software developers, and Service and Agency personnel.

DAD will be a Controlled-Access DII Asset Distribution system in accordance with United States Code, Section 2751, et.seq., and Export Administration Act of 1979 as amended. DAD is restricted for posting classified, budgetary, acquisition, proprietary, or arms information. The primary use of DAD is for the distribution of software and other related reusable electronic assets to authorized users.

A DAD overview graphic is depicted in Figure 1.2.4.2.3-1.

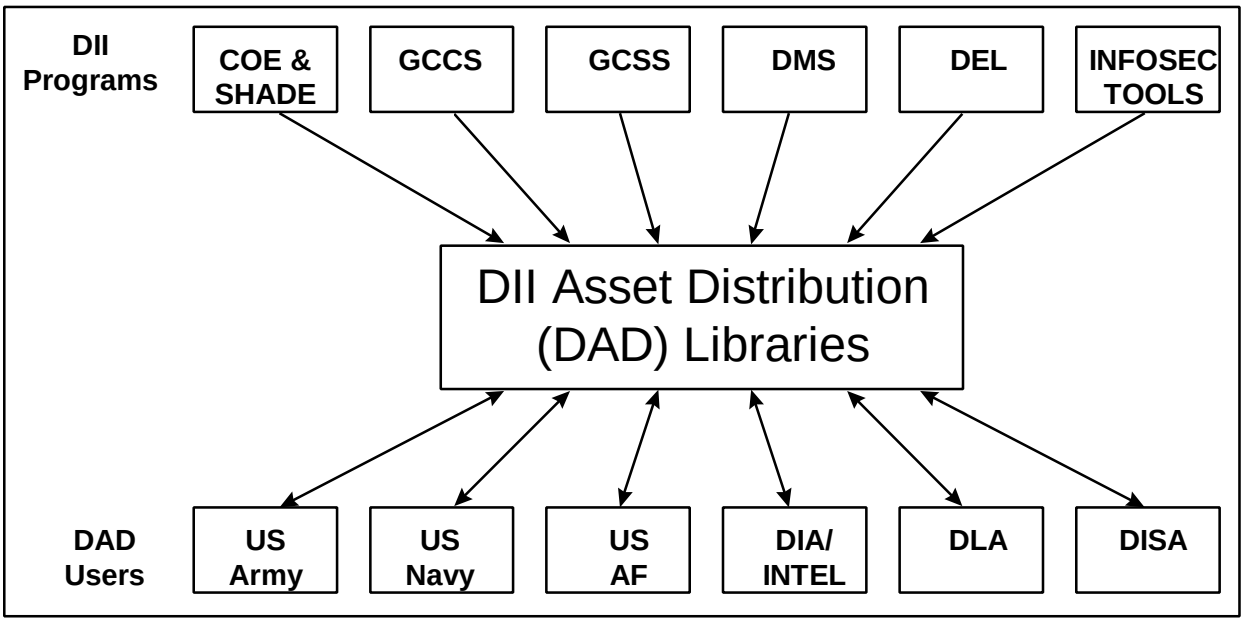

Figure 1.2.4.2.3-1. DII Asset Distribution Overview

1.2.4.2.4 Internal Distribution

CM Services software shall provide automated capabilities for internal distribution of electronic reusable assets within the CFI to engineering, test and integration activities.

1.2.4.2.5 World Wide Web Information Access and Control

CM Services software shall provide automated capabilities for web information access and control to support:

- Posting approved documentation, files and segments on web pages
- Implementing appropriate access controls for assets posted on the web
- Posting information on Global System Problem Reports (GSPRs), software dependencies, segment status, and COTS licenses
- Web information search and query capabilities
- On-line request capabilities for DII COE documentation and software
- Pre-registration of segments, segment prefixes and sockets
- Scheduling of deliveries.

Web information access and control shall be implemented in accordance with applicable DoD and DISA standards and guidelines

1.2.4.2.6 Interface Definition

CM Services software shall provide automated functions for interface definition support, including:

- Identification of DII COE and mission application internal and external interfaces
- Definition of the requirements for DII COE and mission application internal and external interfaces

- Identifying the inputs and outputs of DII COE and mission application internal and external interfaces
- Tracking the decisions and actions of ICWGs.

1.2.4.2.7 Baseline Information

The essential idea of baselines is that in order to plan for, approve, or implement a configuration change, it is necessary to have a definition of the current configuration that is to be changed. Major configuration baselines are the functional, allocated, and product baselines. The functional baseline is defined during the pre-development stage of a CI's life cycle. The allocated baseline (or development configuration) constitutes the current approved performance oriented documentation for a CI to be developed and is established during the development stage. The product baseline constitutes the approved technical documentation that completely describes the functional characteristics, physical characteristics and configuration of a CI during the pre-production and production phases of its life cycle. Each of these major configuration baselines is designated when the given level of the CI's configuration documentation is deemed to be complete and correct, and needs to be formally protected from unwarranted and uncontrolled change from that point forward in its life cycle. CM Services software shall provide automated functions to identify, formally establish, provide access to, and maintain baseline information. Automated baseline information support functions to be provided by CM Services software shall include:

- Traceability of CIs to the specific baseline and product to which they belong
- Identification of DII COE and mission application items to be baselined after successful testing
- Development and implementation of processes with which to capture, maintain, analyze, and report on DII COE and mission application baseline information.

1.2.4.2.8 Controlled Libraries

The functional, allocated and product config uration documentation must be mutually consistent and compatible. The Government needs to take delivery of and control baseline documentation at a level of detail commensurate with the development, production, operational, maintenance and re-procurement strategies for DII COE and systems based on DII COE. Configuration documentation shall be maintained and protected from unauthorized access and changes in controlled libraries. CM Services software shall provide automated functions for controlled libraries to support:

- Identification of the libraries requiring access control
- Identification of the types of access control for the types of controlled libraries
- Identification of the access control mechanism for each type of library maintained
- Identification of the organizations requiring access to the libraries
- Assignment of the required access control mechanism to each organization depending on the types of library and access control
- Identification of the information that needs to be in each of the controlled libraries.

1.2.4.2.9 CI and Tracking Information Access and Control

CM Services software shall provide automated functions for CI and tracking in formation access and control to support:

- Identification of CIs and tracking information that requires access control
- Identification of the types of access control for the types of information maintained
- Identification of the access control mechanism for each type of information maintained
- Identification of the organizations requiring access to that information
- Assignment of the required access control mechanism to each organization depending on the types of information and access control.

1.2.4.2.10 License Management

CM Services software shall provide license management processes to automate support for:

- Single point COTS license management
- Providing on-line access to COTS license information
- License accountability
- License procurement negotiation and planning
- Tracking COTS/segment dependencies.

1.2.4.2.11 Request Processing

CM Services software shall provide asset request processing functions to automate support for tracking the status of and reporting on DII COE asset requests.

1.2.4.2.12 Subscriber Lists

CM Services software shall provide automated capabilities for tracking DII COE subscriber information to support distribution of DII COE assets and determining customer licensing requirements.

1.2.4.2.13 Ad hoc Distribution Lists

CM Services software shall provide automated capabilities for tracking DII COE subscriber information to support ad hoc distribution of DII COE assets and determining customer licensing requirements. Ad hoc distributions apply to DII COE customers that do not receive regular distributions of DII COE assets.

1.2.4.2.14 Change Control - ECP/GSPR/SCN/NOR

Each configuration baseline serves as a point of departure for future CI changes. Each change from the previous baseline to the current baseline occurs through the configuration control process. CM Services software shall provide automated functions for change control process establishment and implementation to manage:

- Engineering Change Proposals (ECPs)
- Global System Problem Reports (GSPRs)
- Specification Change notices (SCNs), and

- Notices of Revision (NORs).

1.2.4.2.15 Version Control

CM version control processes support the management of different versions of configuration items during the development process. Tools for automating version control functions shall provide the capability to develop and build the next version of DII COE products while at the same time, addressing problems in current product releases. CM Services software shall provide automated functions for version control to support:

- Establishment and maintenance of version control numbers for each baselined item
- Development and implementation of processes with which to manage item version control.

1.2.4.2.16 Configuration Control Metrics

CM Services software shall provide automated capabilities for developing and reporting metrics for configuration control processes, to include:

- ECP/GSPR cycle times
- Types of ECPs/GSPRs submitted (e.g., functional areas affected)
- Rate of ECP/GSPR approval
- ECP/GSPR incorporation rates
- Number/percentage of deviation requests
- Number of configuration audits planned, held, successfully completed (all actions), and open actions remaining per audit
- Number of authorized and unauthorized requests for each asset
- Changes to segment processing schedule.

1.2.4.3 Configuration Status Accounting (CSA)

To support Configuration Status Accounting (CSA), automated processes shall be provided for creating and organizing the knowledge base necessary for the performance of configuration management. The purpose of CSA is to provide a highly reliable source of configuration information to support all program/project activities including program management, systems engineering, manufacturing, software development, testing and maintenance, logistic support, modification, and system maintenance.

During the pre-development phase, CSA activities focus on establishment of a common system/database for recording and reporting the status of management and technical decisions, as well as the status of proposed requirement and documentation changes. This data repository evolves to become a key component of the MIS. During the development phase, all CM activities provide information to the status accounting database as a by-product of transactions that take place as the functions are performed. The CSA database collects and maintains information on the as-designed, as-built, as-delivered, or as-modified configuration of any serial-numbered unit of the product. Other information, such as the current status of any change, the history of any change, and the schedules for and status of configuration audits is also maintained and accessible in the database. Controlled access is provided to the digital data, software and documentation

files for each document and software item released for use. During the development and pre-production phases, performance measurement metrics are generated from information in the CSA database and provided to the Management Planning functions for use in monitoring the process and in developing continuous improvements. During pre-production, CSA activities include testing and assuring the integrity of the configuration information in the CSA database. The CSA database becomes a vital reference for timely configuration information to facilitate decision making on changes, deployment of assets, determining applicable replacements, and performing updates/upgrades. The CSA database also provides the status of all critical and major requests for deviation and waivers that affect the configuration of system components/CIs. During the production phase, configuration changes resulting from retrofit and replacements through maintenance action are recorded in the CSA database. In addition, the CSA database continues to track the results of audits, the status of engineering changes, and the decisions and actions of IPTs and ICWGs.

1.2.4.3.1 Data Tracking and Recording

Data tracking and recording requirements evolve over the life cycle of a program. CSA information sources during each of the life cycle phases are summarized below.

a. Pre-development phase information is primarily derived from:

- Mission Need Statements
- Baseline performance/cost/schedule goals
- System requirements documents for alternative configurations
- ECPs or contract change proposals, as applicable
- Preliminary system performance specifications
- Test plans
- Engineering reports.

b. Development phase information is primarily derived from:

- System performance specifications
- CI performance and detailed specifications
- Engineering drawings and associated lists
- Test plans, procedures and results
- Audit plans, reports and certifications
- ECPs, deviation requests, NORs, and SCNs.

c. Pre-production phase information is primarily derived from:

- CI/system detailed performance specifications
- Test plans, procedures and results
- Audit plans, reports and certifications
- ECPs, deviation requests, NORs, and SCNs
- Installation and as-built verification.

d. Production phase information is primarily derived from:

- All development and pre-production phase items
- Current configuration of all Systems/CIs in all locations
- Support equipment and software
- Spares
- Trainers and training material
- Operating and maintenance manuals
- CI delivery dates, licensing data and warrantee data
- Verification/validation and incorporation of retrofit instructions and kits
- Installation of spares and/or replacements by maintenance action.

To support data tracking and recording requirements, automated functions shall be implemented for:

- Identification of the data (information) to be tracked and recorded
- Identification of where the data (information) is tracked and recorded
- Identification of the frequency that the data (information) is collected, recorded, and queried
- Identification of how the data (information) is tracked and recorded
- Identification of who tracks and records the data (information)
- Identification of the volume of data (information) tracked and recorded
- Identification of existing catalogs and templates for re-use possibilities.

1.2.4.3.2 CI and System Status Monitoring

The performance thresholds in top level specifications and program Operational Requirements Documents (ORDs) must be reflected in the system or top level CI specification that constitutes the functional baseline for the program for those thresholds to be achieved. These documented thresholds shall be used by the CM Services software to monitor CI and system performance. Violations of specified thresholds (including conditions specified in waivers) shall be detectable by CM Services software and shall be recorded for further analysis and for determination of whether any corrective actions are required.

1.2.4.3.3 Build List Status (Per Platform)

CM Services software shall provide automated capabilities for tracking and reporting the status of current build lists. Automated support for querying, reporting on, and controlling access to build list information shall be implemented.

1.2.4.3.4 Configuration Change Status

CM Services software shall provide automated capabilities for tracking the status of configuration change requests and proposals. To support configuration change status requirements, automated functions shall be implemented for:

- Reporting on the status of problem reports and change requests and proposals being tracked
- Conducting searches on and querying change status information
- Identifying actions taken to resolve problems
- Identifying fixes targeted for specific releases
- Identifying changes that have already been incorporated.

1.2.4.3.5 Change Accountability

To support change accountability, CM Services software shall provide automated capabilities to support:

- Unique identification of every problem report and change request/proposal reported
- Traceability of all changes
- Linking related and duplicate problems and changes
- Tracking disposition of changes.

1.2.4.3.6 Inventory of Libraries

CM Services software shall provide automated functions for managing the inventory of libraries to support:

- Identification of projected software and document libraries for each build
- Development and implementation of a mechanism to inventory and manage access to those libraries.

1.2.4.3.7 Status Accounting Information Access and Control

CM Services software shall provide access to and control of status accounting information. Automated capabilities shall provide:

- Designation of “Controlled Communities of Interest” and the associated privileges and access permissions
- Controlled access to baseline CI status accounting data and documentation
- Controlled access to status accounting data query and search functions
- Password protection and assignment of user permissions.

1.2.4.3.8 Configuration Status Accounting Metrics

CM Services software shall provide automated functions for developing and tracking configuration status accounting metrics to support:

- Development of potential problem scenarios related to status accounting
- Identification of metrics with which to classify, verify, and validate the potential problems identified from the problem scenarios
- Development and implementation of processes with which to capture, maintain, analyze, and report on status accounting problems

- Development and implementation of processes to alleviate the problems related to status accounting
- Development and implementation of processes with which to evaluate the success of the processes designed to alleviate the problems related to status accounting.

Specific types of metrics used to evaluate status accounting processes include:

- Tracking attributes of problem reports and change requests/proposals
- Comparing system thresholds and actual performance parameters
- Tracking dependency violations.

1.2.4.4 Configuration Audits

Audits ensure the integrity and accuracy of configuration baselines and configuration data repositories used to support configuration control of a product throughout its life cycle. Successful completion of verification and audit activities results in a verified System/CI(s) and a documentation set that may be confidently considered a product baseline. It also results in a validated process to maintain the continuing consistency of product to documentation. During the pre-development phase, audit activities establish the schedule, agenda, facilities and rules of conduct for audits and identify the participants. Pre-development activities also include verifying contractor design solutions. During the development stage, audit activities expand to include performing verification tests on a selected unit or units of CIs and performing repetitive acceptance testing on each deliverable CI. The physical aspect of verification during the development phase establishes that the as-built configuration is in conformance with the as-designed configuration. Once the initial configuration has been verified, approved changes to the configuration must also be verified. During the pre-production phase, configuration audits provide the framework and detailed requirements for verifying that the contractor's development effort has successfully achieved all of the requirements specified in the configuration baselines. During the production phase, physical and functional configuration audits are performed to verify that the actual configuration and performance of system CIs match approved documentation and requirements.

CM Services software shall provide automated processes to track DII COE audit schedules, agendas, facilities and identified participants. Physical and Functional Configuration Audits as well as audits of CM libraries and valid COTS licenses will be supported by CM Services software. Configuration audit records documenting the problems and action items resulting from audits, as well as actions taken, will be maintained and accessible by authorized personnel.

1.2.4.4.1 Site and Configuration Audit Support

CM Services software shall provide automated functions for site and configuration audits to support:

- Tracking audit schedules, agendas, facilities and identified participants
- Comparing the Build Plan with the Build List of each hardware platform
- Recording and tracking discrepancies
- Development of plans to correct discrepancies

- Tracking resolution of identified discrepancies.

1.2.4.4.2 Documentation Library

To support physical and functional configuration audits, the complete set of product baseline documentation shall be identified and accessible. The product baseline documentation includes the complete set of released and approved engineering design documents, such as engineering drawings and associated lists for hardware; and the software, interface and database design documents for software. The product baseline also includes by reference, the material and process specifications invoked by engineering documentation. Automated functions for managing the documentation library support:

- Comparison of the DII COE's and mission application's suite of baselined documents to the suite of "as-built" documents
- Preparation of reports on the results of the comparison
- Coordinating reports and forwarding to the responsible organization
- Development and implementation of corrective measures as required.

1.2.4.4.3 Software Library (Segments / Data)

CM Services software shall provide automated functions for ma naging the software library to support:

- Comparison of the DII COE's and mission application's suite of baselined software, data, and database segment libraries to the suite of "as-built" software, data, and database segment libraries
- Preparation of reports on the results of the comparison
- Coordinating reports and forwarding to the responsible organization
- Development and implementation of corrective measures as required.

1.2.4.4.4 Build List (Per Platform)

CM Services software shall provide automated functions for managing the Build List (per platform) to support:

- Comparison of the DII COE and mission application build list for each platform to the suite of "as-built" software, data, and database segments for that platform
- Preparation of reports on the results of the comparison
- Coordinating reports and forwarding to the responsible organization
- Development and implementation of corrective measures as required.

1.2.4.4.5 Fielded Equipment: Identification of Performance Problems and Firmware

CM Services software shall provide automated functions for managing identific ation of performance problems and firmware for fielded equipment to support:

- Identification of fielded models of hardware platforms and their firmware revision levels
- Collection of problem reports related to hardware platform models and their firmware

- Development and implementation of a process to track the problems
- Development and implementation of a trend analysis process to indicate quality control problems of the hardware and firmware platform vendor
- Forwarding the indicated quality control problems to the hardware/firmware platform vendor and requesting the vendor to identify a corrective plan.

1.2.4.4.6 License Use / Allocation

CM Services software shall provide automated functions for managing license use versus allocation to support:

- Identification of the negotiated software license agreement for each COTS application
- Instantiation of licensing agreements in the form of a manual procedure or an automated mechanism
- Transferring the responsibility of tracking the number of licenses allocated to each applicable intermediate or "using" organization using the manual procedure or automated mechanism
- Development and implementation of a manual procedure or an automated mechanism to track the actual use of each COTS software application
- Development and implementation of a reporting mechanism to relate the number of allocated licenses compared to the actual "use" of the COTS software application
- Development and implementation of a mechanism to ensure "denial of service" does not occur due to the lack of allocated licenses
- Renegotiation of COTS software license agreements as appropriate.

1.2.4.4.7 Distributions Made Last Quarter

CM Services software shall provide automated functions for tracking asset distributions made during the last quarter and support analysis of information on how, how many, when and where assets were distributed during the past quarter. The capability to generate reports on asset distribution information will be provided to support audit planning.

1.2.4.4.8 Current Web Information

CM Services software shall provide automated functions for comparing assets currently available on web pages with assets and information associated with current approved baselines. CM Services software shall provide the capability to identify and report on discrepancies, outdated assets, and invalid web links.

1.2.4.4.9 Functional Audit Test Report Results

CM Services software shall provide automated functions for managing Functional Audit Test Report results to support:

- Comparison of the DII COE's and mission application's Functional Requirements Matrix to the Final Test Report through Quality Assurance
- Preparation of reports on the results of the comparison
- Coordinating reports and forwarding to the responsible organization

- Development and implementation of corrective measures as required.

1.2.4.4.10 CI and System Requirement Cross-Reference

CM Services software shall provide automated functions for cross-referencing CI and system requirements to the test procedures that validate the requirements.

1.2.4.4.11 Physical Audit Test Report Results

CM Services software shall provide automated functions for managing Physical Audit Test Report results to support:

- Comparison of the as-designed configuration build list to the actual system configuration
- Preparation of reports on the results of the comparison
- Coordinating reports and forwarding to the responsible organization
- Development and implementation of corrective measures as required.

1.2.4.4.12 Risk Assessment of Build

CM Services software shall provide automated functions for build risk assessment to support:

- Developing a risk assessment philosophy based on the requirement satisfaction of the DII COE or mission application software and the need of the software to be fielded
- Inclusion of functional, compliance, security, and schedule impact aspects in the risk assessment philosophy
- Development of a risk mitigation philosophy
- Preparation of a Risk Assessment Report detailing the results of the risk assessment and risk mitigation
- Coordination of the Risk Assessment Report and forwarding it to the responsible organization
- Development and implementation of corrective measures as required.

1.2.4.4.13 Test Readiness Review Support

CM Services software shall provide automated functions to support operational test readiness review (OTRR) planning, to include:

- Maintaining a test readiness review checklist
- Providing traceability of test procedure steps to the requirements/capabilities they verify
- Identifying possible COTS licensing issues.

1.2.4.4.14 Configuration Audit Metrics

CM Services software shall provide automated functions for developing and tracking configuration audit metrics. Metrics used to evaluate audit processes include:

- Tracking changes to original audit plans and schedule
- Tracking number of audits planned, held and successfully completed (including action items)
- Tracking the number of open action items and unresolved discrepancies that are past due.

1.3 Document Overview

This document outlines the software capability requirements for DII COE CM Services applications in accordance with the content and format guidance of *Software Requirements Specification (SRS), Data Item Description (DID), Identification Number: DI-IPSC-81433*.

- Section 1 identifies the CM SRS scope and provides an overview of DII COE and DII COE CM.
- Section 2 lists the documents that are applicable to CM and referenced in this document.
- Section 3 lists the total objective set of CM Services functional capability requirements.
- Section 4 identifies the qualification provisions.
- Section 5 defines the traceability methodologies necessary to account for CM requirements.
- Section 6 contains the applicable notes associated with this SRS and DII COE CM.

Distribution of this entire document is authorized to U.S. Government Agencies and their contractors for critical technology as identified on the front cover. Further dissemination of this document will require written approval from the CM TWG Chair. If the requirements traceability identified in section 5 is removed prior to distribution, then the modified document is approved for public release with unlimited distribution. Only the modified document missing section 5 will be posted on the CM page of the DII COE HomePage. The web address is: http://spider.osfl.disa.mil/cm/cm_page.html.

SECTION 2. REFERENCED DOCUMENTS

2.1 DoD and Federal Documents

The following specifications, standards, and handbooks are used to varying degrees to build the foundation of this document. (Uniform Resource Locator (URL) addresses are provided for the references where available.) Unless otherwise specified, the issues of these documents are those listed in the Department of Defense Index of Specifications and Standards (DoDISS) and supplements.

The standards listed below support modern information systems technology and development practices. Since DII COE does not require standard Major Automated Information Systems Requirement Council (MAISRC) development phases, some of the standards were tailored to apply to the COE system foundation.

IEEE/EIA 12207, *Information Technology-Software Life-Cycle Process,* May 1998

MIL-STD-973, *Configuration Management*, 17 April 1992
[http://www.pica.army.mil/infomenu/cmpm/973/default.htm]

MIL-HDBK-61, *Configuration Management Guidance*, 30 September 1997
[http://www.acq.osd.mil/log/lro/cm.html#standards].

ISO 10007, *Quality Management, Guidelines for CM*, 1995

Department of the Army Pamphlet 73-3 , *Software Test and Evaluation Guidelines* Draft, 31 July 1996 [http://www.odusa-or.army.mil/TEMA/ref.htm]

Department of Defense, *The Program Manager's Guide to Software Acquisition Best Practices*, Version 2.1, October 1997 [http://www.spmn.com/]

Electronic Industries Association (EIA) Standard 649 and MIL STD-2549 are being developed. When approved, these standards will replace MIL-STD-973. MIL-STD-498 was cancelled on 27 May 1998. Information regarding software development and documentation is now contained in the Institute of Electrical and Electronics Engineers (IEEE)/Electronics Industries Association (EIA)/American National Standards Institute (ANSI) standard, Joint Standard 016 (J-STD-16).

2.2 DISA Documents

Copies of DII COE documents may be obtained directly from the NIPRNET. The DII COE HomePage can be accessed at http://spider.osfl.disa.mil/dii/. GCCS Documents are only available over the SIPRNET. If a referenced document is not available in electronic downloadable form, then one can submit an on-line request for DII COE documents on the DII COE HomePage. Please check DII COE document listings carefully before entering an electronic document request. Requests for documents will not be processed for those documents that are already available for downloading from the DII COE HomePages. (URL addresses are provided for the references where available.) In the event one does not have NIPRNET access, a written request can be sent to the addresses listed below for DII COE documentation.

DISA

Configuration Management Department
45335 Vintage Park Plaza
Sterling, Virginia 20166-6701

Requests for non-DII COE or non-GCCS documents should be sent to the Office of Primary Responsibility (OPR) identified for each of the other DISA documents. For those unfamiliar with DISA, please contact the DISA Public Affairs at (703) 607-6900 if further assistance is required.

Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specifications, Version 3.0, 1 July 1997, CM-400-01-04 [http://spider.osfl.disa.mil/cm/general.html.new].

Configuration Management Software and Documentation Delivery Requirements, Version 4.0, 4 August 1998, CM-165-60-04 (NOTE: This is used for DII COE and GCCS deliveries to the DISA CFI) [http://spider.osfl.disa.mil/cm/general.html.new].

Defense Information Infrastructure (DII) Common Operating Environment (COE) Developer Documentation Requirements, Version 2.0, 23 January 1998, CM-400-214-04 [http://spider.osfl.disa.mil/cm/general.html.new].

Defense Information Infrastructure (DII) Common Operating Environment (COE) User Interface Specifications, Version 3.0 (includes Style Requirements of DII COE Compliance as Appendix I), 8 March 1998, CM-400-18-05 [http://spider.osfl.disa.mil/cm/general.html.new].

Defense Information Infrastructure (DII) Common Operating Environment (COE) Baseline Specifications, Version 3.1, 29 April 1997, CM-400-25-07 [http://spider.osfl.disa.mil/cm/general.html.new].

Defense Information Infrastructure (DII) Common Operating Environment (COE) How To Segment Guide, Version 4.0, 30 December 1996, CM-400-130-01 [http://spider.osfl.disa.mil/cm/general.html.new].

Department of Defense Technical Architecture Framework for Information Management, Volumes 1-8, Version 3.0, 2 January 1997 [http://www-library.itsi.disa.mil/tafim.html].

System Requirements Specification for the Global Command and Control System (GCCS) & Defense Information Infrastructure (DII) Consolidated Management Information System (CMIS), 19 June 1997.

System Requirements Specification for the Network Management (NM) Functional Area of the Defense Information Infrastructure (DII) Common Operating Environment (COE), Revision 2.0, 8 July 1997, CM-400-260-01 [http://dii-sw.ncr.disa.mil/coe/srs/].

System Requirements Specification (SRS) for Defense Information Infrastructure (DII) Asset Distribution (DAD), Version 1.0, 17 September 1998.

DII COE Security Software Requirements Specification (SRS), Version 3.0, 11 July 1997 [http://dii-sw.ncr.disa.mil/coe/srs/security/ss-srs.pdf].

Configuration Review and Control Board (CRCB) Charter, Version 1.0, June 1997

Architecture Oversight Group (AOG) Charter, Version 1.0, June 1996.

Technical Working Group (TWG) Charter, Version 1.0, June 1996 [http://spider.osfl.disa.mil:81/aog_twg/aog/aog_page.html].

Department of Defense Joint Technical Architecture Draft, Version 2.0, 26 May 1998. [http://www-jta.itsi.disa.mil/jta/jtav2-final-980526/acro.htm].

2.3 Order of Precedence

In the event of a conflict between the text of this document and the documents cited herein, the text of this document takes precedence. However, nothing in this document supersedes applicable laws and regulations unless a specific exemption has been obtained. Please contact the chairperson of the DII COE CM TWG if further clarification is required.

This page intentionally left blank.

SECTION 3. REQUIREMENTS

3.1 Required States and Modes

The CM Services of the DII COE has no operating modes or states of its own since the DII COE is a foundation. However, DII COE-compliant systems do have various modes of operation. The four general modes are:

Operational Mode: This is the normal mode of operation where the DII COE-compliant system is on-line supporting the operational mission of the community of interest.

Maintenance Mode: In this mode, portions of the hardware or software associated with a DII COE-compliant system at a particular site will be off -line for maintena nce, modification, upgrade, or other related actions.

Training Mode: In this mode, a portion of the DII COE-compliant system may be operating with separate databases using simulated inputs in support of training for a portion of the user population of the community of interest. Care must be taken to ensure that exercise data are not mixed with operational data.

Exercise Mode: In this mode, a portion of the DII COE-compliant system may be operated with separate databases using simulated inputs in support of an exercise for a portion of the user population of the community of interest. This could be for war gaming purposes or for testing new functionalities for the community of interest.

It is important to understand these modes of operation are not mutua lly exclusive. In fact, normal day-to-day operations will probably find all four operating modes existing at the same time within different portions of a large-scale DII COE-compliant system. The different modes will be distinguished by administrative features, geographical or architectural boundaries, or management domains. The CM Services requirements are valid for all required states and modes.

3.1.1 DII Asset Distribution (DAD) States and Modes Requirements

Requirements for DAD states and modes are provided in Table 3.1.1-1.

Table 3.1.1-1. DAD States and Modes Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.1.1-1	DAD shall provide multiple modes that can operate concurrently.			
3.1.1-2	DAD shall contain redundancies so that while a portion of DAD is in any mode, other portions of DAD continue to provide full capability in other modes.			
3.1.1-3	DAD shall record and report the dates and times each of the modes is in use, including the specific identity and location of the server used for the mode.			
3.1.1-4	DAD shall provide the capability to schedule the Maintenance, Training and Testing Modes for any specified DAD Server.			
3.1.1-5	DAD shall accommodate Operations Mode. This is the mode of operation where DAD is supporting the operational asset distribution mission.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.1.1-5.1	DAD Operations mode shall be 24 hours per day, 7 days per week.			
3.1.1-5.2	Mechanisms within DAD shall ensure that activities and data used in any other modes is not mixed with and does not affect Operations Mode activities and data.			
3.1.1-6	DAD shall accommodate Maintenance Mode. In this mode, portions of the server hardware or software at one or more sites are offline for maintenance, modification, upgrade, or other related actions.			
3.1.1-6.1	Maintenance mode for any particular server shall not exceed 8 hours in duration.			
3.1.1-7	DAD shall accommodate Training Mode. In this mode, a portion of DAD may be operated with separate databases using simulated inputs in support of training for a portion of the user population.			
3.1.1-8	DAD shall accommodate Testing Mode. In this mode, a portion of the DAD may be operated with separate databases using simulated inputs in support of testing for a portion of the user population.			

3.2 Configuration Management (CM) Services Capability Requirements

This section describes CM Services requirements for CM support capabilities to be available in DII COE-compliant CM support applications. The requirements are based on two primary sources. The first sources of requirements are the published documents pertaining to CM, such as MIL-STD-973 (Configuration Management), ISO 10007 (Quality Management Guidelines for CM), and MIL-HDBK-61 (Configuration Management Guidance). The other sources of requirements are those that come from the various DII COE user community developers and chief engineers that build end systems. Twice a year the DII COE Engineering Office conducts a formal requirements Data Call for desired DII COE capabilities. This call goes out through the voting members of the DII COE Architecture Oversight Group (AOG). Requirements can also be submitted out-of-cycle through the appropriate TWG provided the voting member of the AOG for that Service or Agency approves the submission. For more information on the DII COE schedule consult the COE Engineering Page off of the DII COE HomePage.

This section captures all validated CM Services software requirements submitted to the DII COE Engineering Office through the CM TWG. The CM TWG includes the Asset Distribution Sub-Panel and the Enterprise Licensing Sub-Panel. The Enterprise Licensing Sub-Panel of the CM TWG will support the AOG to leverage DoD's buying power by combining Service/Agency DII COE COTS software requirements for potential enterprise licensing. The Asset Distribution Sub-Panel of the CM TWG identifies, prioritizes and tracks DoD and other agency asset distribution requirements and coordinates implementation of electronic distribution of DII COE and DII COE-compliant assets. Requirements for functions supporting asset distribution are also addressed in the DII COE SRS for the DII Asset Distribution (DAD) System. Overall, each TWG is responsible for tracking and maintaining the requirements for their functional areas.

The CM requirements are subdivided into Management Architecture and Configuration Management (CM) Services Components. Management Architecture requirements address DII

COE and DII COE-based system architectural requirements that are not associated with any particular CM discipline. All of the tables within Section 3.2 stating requirements follow the same format. The first column provides a unique paragraph number that must always be referenced when changes are recommended to existing requirements. All new requirements submitted to the CM TWG will be sorted and assigned paragraph numbers as required. This does not, however, prevent the submitter of requirements from providing a recommendation as to which section the requirement belongs in. The second column is the description of the requirement. The requirement must be clearly and completely described in words that can be understood by non-technical individuals. The CM TWG will work with the submitter to ensure the requirements are properly understood and captured. The third column identifies the DII COE build (or version of software) in which the capability is required. Consult the DII COE HomePage if further detailed scheduling information is required. The fourth column identifies which operating systems, supported by the CM Division, the capability is required for. This column does not specifically address a particular version of an operating system because this is explicitly identified by the DII COE version number. Here it is sufficient to specify Solaris (Sol), Hewlett Packard (HP), or Microsoft NT (NT). The final column is for comments. Organizations who submitted requirements but do not see them listed in this document must work through their Service or Agency representative to the CM TWG to resolve the issue.

3.2.1 Management Architecture

The management architecture section deals with the extremely high level requireme nts of the most basic nature for CM Services. This includes requirements as basic as “CM services will exist” or that “a CM database will exist” for supporting the CM Services.

3.2.1.1 General Architecture Requirements

General architecture requirements for CM Services software are provided in Table 3.2.1.1-1.

Table 3.2.1.1-1. General Architecture Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.1.1-1	Automated DII CM support services shall be provided.		Sol/HP/NT	
3.2.1.1-2	The system shall use client/server technology.			
3.2.1.1-3	DII COE CM tools shall support a distributed architecture such that CM activities can be performed at various hierarchical levels.			
3.2.1.1-4	The system shall provide standardized APIs that support access to system CM functions across a network.			
3.2.1.1-5	CM services shall be interoperable with the goals and structure of the DII.		Sol/HP/NT	
3.2.1.1-6	The system shall be DII COE-compliant at a minimum Level 5, Level 7 by 1999.			
3.2.1.1-7	The system shall be flexible enough to rapidly adapt to changing requirements and workflow.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.1.1-8	CM Services software segments and applications shall comply with the guidelines, specifications and standards defined in the *I&RTS*, the *User Interface Specification*, *DII Software Quality Compliance Plan*, and related documents such as the *Joint Technical Architecture (JTA)*.			
3.2.1.1-9	The system shall be able to operate on all platforms and client/server environments currently supported by the DII COE.			
3.2.1.1-10	The systems shall be capable of running on the 486 and Pentium PCs available to the average DISA user. The minimum configuration available to the average DISA user is an i486 processor running at 33 MHz, with 16 MB of RAM and a 433 MB disk drive using Windows NT 4.0 as the operating system.			
3.2.1.1-11	The system shall be interoperable with all platforms and client/server environments currently supported by the DII COE.			
3.2.1.1-12	The system shall be scalable so that it can support changing architectures without losing functionality.			
3.2.1.1-13	The system shall be Year 2000 (Y2K) compliant. Y2K compliance shall be based on the Federal Acquisition Regulation (FAR) 48 CFR Parts 39.002 and 39.106. System software shall process dates in the DoD standard format YYYYMMDD, and alternately use a bridge or filter technique to reconcile non-standard format dates passed across interfaces.			
3.2.1.1-14	Software developed to support the system shall comply with the development environment processes and conventions described in Chapter 9 of the I&RTS.			
3.2.1.1-15	System development shall be performed with development tools compatible with the Oracle core database.			
3.2.1.1-16	System development shall be done using 4GL and 5GL tools to maximize productivity (3GL tools may be necessary in some limited circumstances but use should be minimized).			
3.2.1.1-17	The system shall be installable on any user's PC without incurring additional software licensing costs.			
3.2.1.1-18	The system manager shall be able to monitor system performance. Monitoring the system operational condition shall be supported by visual displays concerning the status of critical system operating parameters (queue size, software modules executing, etc.)			
3.2.1.1-19	The system shall provide the system manager the capability to start on-line diagnostics or to run background diagnostics when the system is not actively engaged in operational processing.			
3.2.1.1-20	The system shall provide utility programs to support system managers in the maintenance of system files and databases.			
3.2.1.1-21	The system shall enable the creation of user account groups and roles by a Security Manager or System Administrator.			
3.2.1.1-22	The system shall provide the System Administrator with the capability to create and to restore backup tapes.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.1.1-23	The system shall provide the System Administrator with the capability to configure network host tables.			
3.2.1.1-24	The system shall provide the System Administrator with the capability to configure and manage the network.			
3.2.1.1-25	The system shall provide the System Administrator with the capability to shutdown and to reboot the system.			
3.2.1.1-26	The system shall have the ability to automatically notify pre-designated persons whenever certain pre-defined events occur and shall have a facility for managing those events and the person(s) associated. For example, CM needs to be notified when new problem reports (PRs) created by outside users have been placed in an intermediate table in order to facilitate the timely entry of the GSPR into the database and the coordination of assigned control numbers with the originator.			
3.2.1.1-27	The system shall provide event alerts that attract user attention to system operational problems.			
3.2.1.1-28	The system shall provide event alerts that indicate user errors in data entry or program execution.			
3.2.1.1-29	The system shall provide alerts that inform the user and system manager of each detected equipment or software malfunction.			
3.2.1.1-30	When an alert status occurs, the system shall require user action to clear/acknowledge the alert.			
3.2.1.1-31	The system shall allow users to enter/modify data from their desktop PCs.			
3.2.1.1-32	The system shall be able to import data from other DII COE CM tools.			
3.2.1.1-33	The system shall effectively support the use of third-party data extraction tools for unique requirements. Examples of such tools include Clear Access and Crystal Reports.			
3.2.1.1-34	The system shall be able to compare/contrast data with similar datasets from other DII COE CM systems to allow for consistency and verification checking.			
3.2.1.1-35	The system shall support multiple, simultaneous hierarchical organizational structures for reporting and information exchange interfaces.			
3.2.1.1-36	The system shall use a consistent design style and follow industry standards for interface design.			
3.2.1.1-37	CM tools shall provide application program interfaces (APIs) that permit easy and flexible extensions to management.		NT	
3.2.1.1-38	CM Applications shall be able to share their management information repositories and to support common management operations upon such repositories.		Sol/HP/NT	
3.2.1.1-39	The system shall be able to interoperate with and share system data with other DII COE CM system applications across a network.			
3.2.1.1-40	The system shall maximize the use of predefined list box data fields to promote data consistency and ease-of-use.			
3.2.1.1-41	DAD shall be provided.			
3.2.1.1-42	DAD shall be congruent with the goals and structure of the DII.			
3.2.1.1-43	DAD shall have the capability to generate composite views of DAD resources and services.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.1.1-44	DAD shall be scalable.			
3.2.1.1-45	DAD shall provide the capability to electronically receive, manage, store, and distribute DII assets.			
3.2.1.1-46	DAD shall provide the capability to track the life-cycle status of each asset.			
3.2.1.1-47	DAD shall be a Controlled-Access DII Asset Distribution system in accordance with United States Code 2751, et.seq. and Export Administration Act of 1979 as amended.			
3.2.1.1-48	The system shall provide the capability to automate software distribution across a network.			
3.2.1.1-49	The system shall provide the capability to automate software installation and updates across a network.			

3.2.1.2 Database Architecture Requirements

DISA will controll the configuration of DII COE CIs in the Management Information System (MIS) database that will consolidate and control all configuration items and verify receipt of documentation and CIs. The products from this process will be reports and/or access to the baseline data. Database architecture requirements for CM Services software are provided in Table 3.2.1.2-1.

Table 3.2.1.2-1. Database Architecture Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.1.2-1	The system shall use Open Database Standards, including structured query language (SQL), for database updates and queries.			
3.2.1.2-2	The system shall be developed using an SQL standard language.			
3.2.1.2-3	The system shall comply with Open DataBase Connectivity (ODBC) standards and provide ODBC interfaces.			
3.2.1.2-4	DII COE CM tools shall not use proprietary databases to store CI data.			
3.2.1.2-5	The system shall be developed using a relational database model under the Oracle Relational Database Management System (RDBMS).			
3.2.1.2-6	The system shall be able to interface with (read and/or write to) other databases used in CFI process management such as the site hardware/software database and the DII Hot Line database (HRR System).			
3.2.1.2-7	System databases and applications accessing databases shall conform to the COE database server environment so they do not bypass its features.			
3.2.1.2-8	The system shall be able to update, receive updates from, and share system data with a central DII COE CM system data repository across a network.			
3.2.1.2-9	DII COE CM tools shall store any common data to a predefined standard RDBMS in such a manner that it can be easily shared with other software.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.1.2-10	To the maximum extent possible, system segments and applications shall take advantage of and share objects belonging to other databases as found within the Shared Data Environment (SHADE) repository.			
3.2.1.2-11	The MIS shall ensure the referential integrity of the data such that changes to unique data elements shall only have to be made in one place and the change will cascade throughout the data repository.			
3.2.1.2-12	The system shall prevent write conflicts and write-read conflicts to the database by multiple users accessing the same records.			
3.2.1.2-13	Definitions of system segment and application schema components shall be included in the system DBMS data dictionary. Definitions of segment data stores, tables, elements, stored procedures, and views shall be stored in the system's data dictionary tables as comments.			
3.2.1.2-14	Data element names shall comply with DoD standards from the DoD Data Model (DDM) and Defense Data Dictionary System (DDDS) where applicable.			
3.2.1.2-15	Names of data stores (i.e., DBMS-managed components of a database segment) to be used by the system, which can be data, indices, or static data, shall have a maximum of 30 characters (uppercase letters, numbers, and underscores) and shall follow the naming conventions appropriate to the type of data as follows: <segment prefix>_DATA <segment prefix>_INDEX <segment prefix>_STATIC			
3.2.1.2-16	Database table names shall be meaningful and have a maximum of 26 characters (uppercase letters, numbers, and underscores). If Oracle database snapshots are being used for data replication services for other sites, table names should be limited to 20 characters.			
3.2.1.2-17	No reserved words may be used in table names.			
3.2.1.2-18	System software provided by developers shall only create tables in storage areas created by and belonging to the application database segment.			
3.2.1.2-19	Database views shall be able to be queried, updated, inserted into, and deleted from, with appropriate restrictions.			
3.2.1.2-20	Database view names shall be meaningful and have a maximum of 30 characters (uppercase letters, numbers, and underscores).			
3.2.1.2-21	Updateable views shall comply with the restrictions described in the I&RTS, Paragraph 4.3.4.3.			
3.2.1.2-22	Data types used shall not be machine-dependent (e.g., float). See Table 3.2.1.2-2 for data types available in a specific DII COTS DBMS and that are machine independent.			
3.2.1.2-23	The system shall comply with the rules on database objects, including constraints, stored procedures, triggers, and indices, as described in Paragraph 4.3.4.4 of the I&RTS.			
3.2.1.2-24	CM databases shall be capable of being distributed in order to meet database robustness requirements affected by communication outage characteristics.		Sol/HP/NT	

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.1.2-25	The system shall allow the user to display the percentage of the MIS database currently in use.			
3.2.1.2-26	The system shall provide the capability for the creation, storage, modification, deletion and control of database query filter packages (canned queries).			
3.2.1.2-27	The system shall provide the user with assistance for constructing valid queries to the system's RDBMS.			
3.2.1.2-28	The users shall have the following output medium options when performing a query: display, print, display/print.			
3.2.1.2-29	The system shall provide web-based access to database query filter packages.			
3.2.1.2-30	The system shall provide the Database Administrator (DBA) with the capability to archive and restore database tables.			
3.2.1.2-31	The system shall include a mechanism for archiving obsolete records out of the active database. Such a mechanism must maintain a residual record verifying the existence of the record, a pointer to where the archived record resides, and the ability to retrieve and recreate the archived record with all information intact.			
3.2.1.2-32	The system shall provide the DBA with the capability to checkpoint and journal database transactions.			
3.2.1.2-33	The system shall provide the DBA with the capability to import and export database entries.			
3.2.1.2-34	The system shall provide the DBA with the capability to create/modify database user accounts.			
3.2.1.2-35	A copy of the MIS database backups shall be kept in a location physically separated from the server site.			
3.2.1.2-36	Full MIS software and data backups shall be done weekly with daily delta backups.			
3.2.1.2-37	The MIS database recovery plan shall be tested.			
3.2.1.2-38	Except in specific instances where it's necessary to preclude access, all MIS users shall have read access to all database objects.			
3.2.1.2-39	The system shall be able to rapidly generate custom reports containing dynamic combinations of fields, based on any combination of selection criteria, and sorted on any field. This will be done through the use of third-party query tools.			
3.2.1.2-40	The system shall include a report generator that shall provide for display or print of the database searches using a database query language.			
3.2.1.2-41	The CM administrator shall be able to select the criteria upon which pre-programmed and ad hoc, on-demand, real-time, and historical outputs can be created.		Sol/HP/NT	

Table 3.2.1.2-2 provides a cross reference of Informix, Oracle, and Sybase data types.

Table 3.2.1.2-2. Database Data Type Cross Reference

Sybase	Oracle	Informix	Range
Integers:			
smallint	smallint	smallint	32,767 to -32,768
int	int	int	2^{31}-1 to -2^{31}
Decimals:			
numeric(p,s)	number(p,s)	numeric(p,s)	10^{38}-1 to -10^{38}
decimal(p,s)	number(p,s)	decimal(p,s)	10^{38}-1 to -10^{38}
float(p)	float(b)	float(p)	machine-dependent
double precision	double precision	double precision	machine-dependent
real	real	real	machine-dependent
Date/Time:			
datetime	date	datetime	valid to seconds only
Character:			
char(n)	char(n)	char(n)	255 chars or less, fixed length
varchar(n)	varchar(n)/varchar2(n)	varchar(n)	255 chars or less, variable length
nchar	nchar	nchar(n)	255 chars or less, fixed length
nvarchar	nvarchar	nvarchar(n)	255 chars or less, variable length
text(n)	long(n)	text	2^{31}-1 chars or less
Binary:			
image	raw	byte	2^{31}-1 bytes

3.2.2 Configuration Management (CM) Services Components

The CM Services components are the basic building blocks that make up the overall CM Services architecture. The components are categorized by CM discipline and then broken into the applicable functional areas. The paragraphs that follow identify the DII COE CM Services component requirements.

3.2.2.1 Configuration Identification and Selection Requirements

3.2.2.1.1 Requirement Definition and Traceability Requirements

Requirements tracing is an integral part of centrally controlling the requirements in the DII COE system. It should be initiated during pre-development configuration identification and follow through to audit processes. Requirements are traced from the moment they come into DII COE management processes through the various DISA DII COE TWGs, into DISA CM, test and engineering (based on versions) and then back through DISA CM to release. In addition, if an automated system is utilized, it may make sense to allow the Services/Agencies to track their requirements prior to receipt by DISA to allow DISA to plan for incoming requirements.

The trace should include system objectives, system requirements and interface requirements, and should start at the highest level and eventually proceed down the hierarchy to the eventual computer program (segment/version) and to test procedures and test reports. Traceability assures all requirements have been mapped into computer program requirements, no new requirements have been introduced that are not directly traceable to or derived from the

system requirements, all input data sources have been specified, and no extraneous outputs have been specified. Tracing the requirements into (and through) test is important because it helps guarantee that testing verifies each and every software and interface requirement. This traceability can be handled manually or by using an automated requirements traceability analysis tool. Automated tools are often most cost-effective and more reliable than manual analysis on complicated systems.

Requirement definition and traceability requirements for CM Services software are provided in Table 3.2.2.1.1-1.

Table 3.2.2.1.1-1. Requirement Definition and Traceability Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.1-1	Requirements for the DII COE shall describe and specify functional requirements.			
3.2.2.1.1-2	Requirements for DII COE shall be able to be added, modified (further detailed), or deleted.			
3.2.2.1.1-3	Requirements for the DII COE shall be tracked.			
3.2.2.1.1-4	Requirements for the DII COE shall be tracked starting when the requirement is initially submitted.			
3.2.2.1.1-5	Requirements for the DII COE shall be tracked when requirement disposition is specified, solution is identified to be GOTS software development, or selection of COTS software implementation.			
3.2.2.1.1-6	Requirements for the DII COE shall be tracked through requirement testing.			
3.2.2.1.1-7	Requirements for the DII COE shall be tracked into DII COE Build Plans/Lists.			
3.2.2.1.1-8	Requirements for the DII COE shall be tracked, finally, into a specific DII COE release.			
3.2.2.1.1-9	A process to manage DII COE software requirements traceability shall be developed.			
3.2.2.1.1-10	DII COE software requirements shall be traceable.			
3.2.2.1.1-11	DII COE software requirements shall be traced from submission.			
3.2.2.1.1-12	DII COE software requirements shall be traced to disposition.			
3.2.2.1.1-13	The system shall provide traceability of requirements to the DII COE Build Plans that partially and/or fully implement the requirement. Requirement traceability shall be supported to the capability(s) and segment(s) in the build plan that implement the requirement.			
3.2.2.1.1-14	DII COE software requirements shall be traced to solution identification via GOTS or COTS software.			
3.2.2.1.1-15	DII COE software requirements shall be traced to testing.			
3.2.2.1.1-16	DII COE software requirements shall be traced to integration.			
3.2.2.1.1-17	DII COE software requirements shall be traced to production (DII COE Version).			
3.2.2.1.1-18	DII COE software requirements traceability shall be automated.			
3.2.2.1.1-19	Using automated means, DII COE software requirements traceability shall be captured.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.1-20	Using automated means, DII COE software requirements traceability shall be maintained.			
3.2.2.1.1-21	Using automated means, DII COE software requirements traceability shall be queried.			
3.2.2.1.1-22	Using automated means, DII COE software requirements traceability shall be output in the form of reports.			
3.2.2.1.1-23	DII COE CM tools shall provide sites with the ability to track their DII COE CIs from the requirement stage until the retirement stage.			
3.2.2.1.1-24	The system shall ensure that all requirements are assigned to a TWG.			
3.2.2.1.1-25	The system shall provide traceability of requirements to the following technical documentation, as appropriate: a. Mission Needs Statement (MNS) b. Operational Requirements Document (ORD) c. User's Functional Description (UFD) d. Operational Concept Description (OCD) e. System/Subsystem Specification (SSS) f. Interface Requirements Specification (IRS) g. Software Requirements Specification (SRS) h. Software Design Description (SDD) i. Interface Design Description (IDD) j. Database Design Description (DBDD) k. Software Product Specification (SPS) l. Engineering Change Proposal (ECP)			
3.2.2.1.1-26	The system shall provide traceability of high level requirements cited in the MNS and ORD to low level requirements.			
3.2.2.1.1-27	The system shall provide traceability of low level requirements to the high level requirements cited in the MNS and ORD.			
3.2.2.1.1-28	The system shall provide traceability of requirements to the following test documentation, as appropriate: a. Test and Evaluation Master Plan (TEMP)/Test and Evaluation Plan (TEP) b. Detailed Test Plan (DTP) c. Software Test Plan (STP) d. Software Test Description (STD) e. Software Development Files (SDF)			
3.2.2.1.1-29	The system shall be able to link functional and interface requirements to documented system objectives, the DII COE segment(s) version(s) satisfying the requirements, and test procedures that verify implementation of the requirement in DII COE software.			
3.2.2.1.1-30	The system shall require that new requirements be traceable to the originating source, whether they are derived from existing system requirements, Service/Agency requirements input in response to Data Calls, or introduced through proposed DII COE system enhancements or improvements.			
3.2.2.1.1-31	All requirements for application data inputs and outputs shall be specified and traceable to the requirement source.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.1-32	The system shall provide the capability to generate and distribute a Data Call form for soliciting new DII COE requirements from users. The Data Call form shall request the following information: a. Requestor Organization b. Date Submitted c. Data Call Date d. Point-of-Contact Name/Phone/Fax/Job Title/Email Address e. Requirement Description f. Requirement Type g. DII COE Area of Responsibility (e.g., Communications, Network Management, etc.) h. Affected system program i. Desired DII COE Build j. Targeted Operating System (OS) k. DII COE Engineering Disposition l. Need Date m. Comments			
3.2.2.1.1-33	The system shall provide automated electronic import of requirements and associated information from completed Data Call Forms into the requirements database.			
3.2.2.1.1-34	Requirement information tracked by the system shall include requirement attributes gathered during data calls as well as the following: a. Requirement Tracking Number b. Assigned Product Number c. Assigned Product Release d. Assigned Product Version e. Assigned Segment Identification (ID) f. Assigned DII COE Release g. Assigned Date of Release h. Assigned Developer i. Estimated Cost to Implement			
3.2.2.1.1-35	The system shall provide flexible, column-based displays of system requirements for which the user is able to select which attributes to display and to set up default views of requirements data.			
3.2.2.1.1-36	The system shall provide the capability to display system requirements information in graphical format, such as displaying requirements attributes as bar charts alongside the requirements to which they apply.			
3.2.2.1.1-37	The system shall provide the capability to identify potential duplicate requirements.			
3.2.2.1.1-38	The system shall provide the capability to link duplicate requirements.			
3.2.2.1.1-39	The system shall provide the capability to query requirements data and use filters for viewing system requirements information, such as viewing only high-priority requirements.			
3.2.2.1.1-40	The system shall provide the capability to generate and output formatted and ad hoc reports on system requirements data. The system shall provide the capability to export reports to Microsoft Office, FrameMaker and HTML.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.1-41	The system shall provide automated electronic import of requirements and associated information from Software Requirements Specifications (SRSs).			
3.2.2.1.1-42	The system shall provide the capability to import documents from industry standard applications such as Microsoft Office and FrameMaker and shall retain structured information, formatting and graphics. Import of the following types of files shall be supported: a. Rich Text Format (.rtf format) b. Comma delineated files and spreadsheets (.csv and .tsv formats) c. Microsoft Project files (.mpx format) d. Pictures and Graphics (.OLE and .eps formats)			
3.2.2.1.1-43	The system shall provide traceability of all system requirement changes, including changes to the requirement statements and changes to key requirement attributes.			

3.2.2.1.2 Management Planning Requirements

Management planning requirements for CM Services software are provided in Table 3.2.2.1.2-1.

Table 3.2.2.1.2-1. Management Planning Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.2-1	DII COE Management Planning shall specify each management process necessary for planning functions.			
3.2.2.1.2-2	DII COE Management Planning shall specify each management process necessary for gathering requirements.			
3.2.2.1.2-3	DII COE Management Planning shall specify each management process necessary for tracking requirement submission, disposition, solution, testing, and implementation (DII COE Version).			
3.2.2.1.2-4	DII COE Management Planning shall specify each management process necessary for DII COE software and documentation CM.			
3.2.2.1.2-5	DII COE Management Planning shall specify each management process necessary for management of subordinate management boards and groups, and technical working groups and subpanels.			
3.2.2.1.2-6	DII COE Management Planning shall specify a management structure for the management of planning functions.			
3.2.2.1.2-7	DII COE Management Planning shall specify a management structure for the management of gathering requirements.			
3.2.2.1.2-8	DII COE Management Planning shall specify a management structure for the management of tracking requirement submission, disposition, solution, testing, and implementation (DII COE Version).			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.2-9	DII COE Management Planning shall specify a management structure for the management of DII COE software and documentation CM.			
3.2.2.1.2-10	DII COE Management Planning shall specify a management structure for the management of subordinate management boards and groups, and technical working groups and subpanels.			
3.2.2.1.2-11	DII COE Management Planning shall include the allocation of resources.			
3.2.2.1.2-12	DII COE Management Planning shall include the allocation of resources for the management of gathering requirements.			
3.2.2.1.2-13	DII COE Management Planning shall include the allocation of resources for the management of tracking requirement submission, disposition, solution, testing, and implementation (DII COE Version).			
3.2.2.1.2-14	DII COE Management Planning shall include the allocation of resources for the management of DII COE software and documentation CM.			
3.2.2.1.2-15	DII COE Management Planning shall include the allocation of resources for the management of subordinate management boards and groups, and technical working groups and subpanels.			
3.2.2.1.2-16	The system shall provide the capability to track and report on all selected configuration items.			
3.2.2.1.2-17	The system shall provide the capability to track and report on all changes made to selected CIs.			
3.2.2.1.2-18	The system will provide a CI tracking system with report generation capabilities.			
3.2.2.1.2-19	The system shall provide the capability to generate specialized CI data reports on CIs being tracked based on data content and search criteria and definition of report format.			
3.2.2.1.2-20	The system shall identify and provide access to all current DII COE documentation on CM policies, processes, procedures, methods, records, reports and forms.			
3.2.2.1.2-21	The system shall identify all DoD and Military Standards applicable to current DII COE CM policies, processes, procedures, methods, records, reports and forms. If available, the system shall also provide links to the actual standards and/or provide Uniform Resource Locator (URL) codes that can be used to access the document for on-line viewing or download.			
3.2.2.1.2-22	The system shall allow an automated mechanism for software developers to pre-notify the CM staff of impending segment deliveries. Such notification will allow entry into the database of all data elements currently contained in the Segment Delivery Letter .			
3.2.2.1.2-23	The system shall provide the capability to track information and reporting elements provided in Cost and Schedule Status Reports submitted by each contractor reporting to the DII COE Programs. The system shall maintain a historical file of the information provided in each report.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.2-24	The system shall have the capability to track and maintain distribution codes assigned to all known recipients and addressees for distribution of DII COE assets. Access to DII COE data shall be limited in accordance with the applicable distribution codes, as well as by data rights, Contract Data Requirements List (CDRL) distribution, security requirements, and data status level (released, submitted or approved).			
3.2.2.1.2-25	For each Technical Working Group (TWG) action item officially established by the Government, the MIS shall establish and keep current a separate record to identify: a. The type of TWG b. The identification number of the action item c. Short title for the action item d. The date the action item was established e. For each activity identified as required to close out the action item, provide: (1) Identification of the activity (2) Identification of the responsible agency (3) The suspense date for completion of the activity (4) The actual closeout date of the activity.			
3.2.2.1.2-26	The system MIS shall track all action items that are established during Program Management and System Engineering IPTs. The MIS shall contain general information about the action item and shall track specific activities and suspenses associated with closing the action item.			
3.2.2.1.2-27	For each Program Management /System Engineering IPT action item officially established by the Government, the MIS shall establish and keep current a separate record to identify: a. The type of IPT b. The identification number of the action item c. Short title for the action item d. The date the action item was established e. For each activity identified as required to close out the action item, provide: (1) Identification of the activity (2) Identification of the responsible agency (3) The suspense date for completion of the activity (4) The actual closeout date of the activity.			
3.2.2.1.2-28	The system shall have the capability to track and report on new/proposed system interfaces, both internal and external, and track the approval/disapproval status of the interfaces.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.2-29	For each new/proposed system interface, the system shall record the following information: a. The organization(s) or developer(s) responsible for the items to be interfaced b. The acquisition activity(s) responsible for the items to be interfaced c. Whether the new/proposed interface is at the system, CI, assembly, or part level d. Type(s) and complexity of technical interface attributes; e.g., data, control, frequency, hardware, installation, transmission rate, capacity, etc. e. Developmental status of the items to be interfaced.			

3.2.2.1.3 Configuration Item (CI) Identification Requirements

CI identification requirements for CM Services software are provided in Table 3.2.2.1.3-1.

Table 3.2.2.1.3-1. CI Identification Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.3-1	DII COE Configuration Items (CIs) shall follow an approved identification process.			
3.2.2.1.3-2	CI descriptions shall include the identification of the CI processes that need to be tracked and managed.			
3.2.2.1.3-3	The mechanism(s) to track and manage CI processes shall be identified and planned for.			
3.2.2.1.3-4	The system shall provide Internet access to CI data.			
3.2.2.1.3-5	The system shall identify the current approved configuration documentation and configuration identifiers associated with each CI.			
3.2.2.1.3-6	If a CI is changed, the original CI and the modified CI shall each be uniquely identified.			
3.2.2.1.3-7	A modified CI shall be traceable to the original CI.			
3.2.2.1.3-8	The system shall provide the capability to apply filters and to conduct searches to identify CIs that meet specified criteria and conditions and output the results in a user-specified output format.			
3.2.2.1.3-9	The system shall be made up of the CIs listed in (TBD).			
3.2.2.1.3-10	DII COE COTS and GOTS software shall contain a predefined software signature embedded into its configuration files so that the software can be identified once loaded on a DII COE System.			
3.2.2.1.3-11	The system shall provide a Configuration Item (CI) identification facility to detect, read and store software signatures (i.e., unique identifiers) embedded in CI configuration files that have been loaded on a DII COE system.			
3.2.2.1.3-12	The system shall enable the user to perform an automatic update of site software CI inventory data using the CI software signature data report generated on the site's DII COE system.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.3-13	The system shall provide the capability to detect loaded software executables using defined software signatures.			
3.2.2.1.3-14	The system shall categorize software segments by name (both long and short versions), abbreviation, version number, hardware platform, operating system version, projected release, actual release(s), developer, developer type (COTS/Contract/GOTS/ etc.).			
3.2.2.1.3-15	The system shall provide a functional description of all segments applications being tracked and maintained by the system.			
3.2.2.1.3-16	The system shall be able to record all of the User IDs (UID), Group IDs (GID), and Transmission Control Protocol (TCP) and Universal Datagram Protocol (UDP) Sockets required by a segment.			
3.2.2.1.3-17	The system shall be able to provide a report of all Socket IDs currently in use, all IDs reserved for future use, and all those not in use.			
3.2.2.1.3-18	DII COE CM tools shall provide a graphical depiction of systems with a drill-down capability.			
3.2.2.1.3-19	The system shall be able to create, maintain and update concise hierarchical DII COE system architectural diagrams, depicting the system configuration at various levels of detail, from the overall DII COE system overview down to the lowest replaceable unit for each hardware and software CI.			
3.2.2.1.3-20	The system shall support a web-based capability to publish site architectural diagrams and the associated CI data that supports them.			
3.2.2.1.3-21	The system shall provide the capability for automated collection of configuration information from DII COE-based system workstations. This information collection shall be able to be performed without any intervention from the local administrator.			
3.2.2.1.3-22	Configuration information collected from DII COE-based system workstations shall be able to be compared to the appropriate baseline, the previously recorded configuration for that workstation, and the license database for license compliance.			
3.2.2.1.3-23	If discrepancies are found while comparing workstation configuration information with the current baseline and the license database, an alert shall be sent to the administrator that identifies the workstation(s) and the discrepancies.			
3.2.2.1.3-24	The system shall maintain a listing of Y2K compliant CIs.			
3.2.2.1.3-25	The system shall provide the means to collect system Y2K data to compare to Y2K compliant CIs.			

3.2.2.1.4 Build Plan Support Requirements

Build plan support requirements for CM Services software are provided in Table 3.2.2.1.4-1.

Table 3.2.2.1.4-1. Build Plan Support Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.4-1	The DII COE Build Plan support requirements shall be provided.			
3.2.2.1.4-2	The DII COE Build Plan support requirements shall include the identification of Build Plan management processes.			
3.2.2.1.4-3	The DII COE Build Plan support requirements shall include the specification of a management structure for each management process.			
3.2.2.1.4-4	The DII COE Build Plan support requirements shall include selection methodology of DII COE requirements to be met for each Build Plan generation.			
3.2.2.1.4-5	The DII COE Build Plan support requirements shall include coordination processes with the appropriate DISA Engineering and Configuration Management offices.			
3.2.2.1.4-6	The system shall provide the capability to track information and the individual data elements provided in DII COE Build Plans and generate formatted and ad hoc reports on information and data elements maintained in DII COE Build Plans, both proposed and approved.			
3.2.2.1.4-7	The system shall provide support for generation, modification and update of DII COE Build Plans.			
3.2.2.1.4-8	The system shall provide the capability to maintain historical records on DII COE Build Plans.			

3.2.2.1.5 License Planning Requirements

License planning requirements for CM Services software are provided in Table 3.2.2.1.5-1.

Table 3.2.2.1.5-1. License Planning Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.5-1	The system shall maintain information on all COTS licenses currently required for each DII COE software release. Information maintained on COTS licenses shall include: a. Vendor's products covered in each license b. Types of licenses available c. License terms, conditions and restrictions d. Whether license is transferable e. Products not covered by the license f. Platforms supported g. Instructions for ordering the end-item or product h. Description of the product delivery mechanism i. Instructions on how to get product documentation j. Training Information k. License/Product cost l. End user support and system services offered m. License acquisition vehicle n. Availability of enterprise licensing.			
3.2.2.1.5-2	The system shall identify all licensing agreements and the CIs to which each applies.			
3.2.2.1.5-3	The system shall maintain templates and electronic forms for DII COE Service/Agency COTS License Usage Memoranda of Agreement (MOAs)/Memoranda of Understanding (MOUs).			
3.2.2.1.5-4	The system shall maintain customer profile information for determining the COTS licensing requirements of primary DII COE system customers and Service/Agency distribution points for DII COE software. Information maintained on customer licensing requirements shall include: a. Number of users for each licensed product b. Type(s) of license required c. Customer Point-of-Contact d. Funding source e. Type of DoD Network (Secret, etc.) f. Support services required (Maintenance, distribution, upgrades, technical support, etc.)			
3.2.2.1.5-5	The system shall be able to identify allocated COTS licenses that will expire within 60 and 120 days. The system shall provide the capability to generate an Expiring License Summary Report that will include a list of the COTS licenses, or associated maintenance agreements, by project/user organization, that will expire in the selected timeframe (either <=60 days, or <=120 days). The list will include the product version/revision, vendor, platform, license expiration date, maintenance agreement expiration date and Point-of-Contact information (name, phone, organization, address, etc.)			

3.2.2.1.6 Segment Prefix/Segment/Socket/UID-GID Registration Requirements

Segment Prefix/Segment/Socket/User ID (UID)-Group ID (GID) registration requirements for CM Services software are provided in Table 3.2.2.1.6-1.

Table 3.2.2.1.6-1. Segment Prefix/Segment/Socket/UID-GID Registration Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.6-1	Solutions to DII COE requirements shall be developed in the form of Segments as described in the DII COE *Integration and Runtime Specification (I&RTS)*.			
3.2.2.1.6-2	As directed in the I&RTS, Segments shall be registered with DISA.			
3.2.2.1.6-3	Registration information will be collected in the form of catalog databases.			
3.2.2.1.6-4	Registration catalog databases shall be able to be queried.			
3.2.2.1.6-5	Reports shall be able to be generated based on the segment information submitted.			
3.2.2.1.6-6	Registration information to be collected on each Segment shall be stored in the Registration catalog database and the MIS.			
3.2.2.1.6-7	Registration information to be collected on each Segment shall include Segment Prefix name.			
3.2.2.1.6-8	Registration information to be collected on each Segment shall include Segment programmatic information as specified by DISA.			
3.2.2.1.6-9	Registration information to be collected on each Segment shall include Segment-unique Transmission Control Protocol (TCP) and Universal Datagram Protocol (UDP) socket usage.			
3.2.2.1.6-10	Registration information to be collected on each Segment shall include Segment-unique User Identification (UID) and Group Identification (GID) usage.			
3.2.2.1.6-11	Segment registration information shall be updated as required.			
3.2.2.1.6-12	The system segment registration process shall allow users to enter new, unique segment prefix codes and the supporting data regarding the application/system being proposed for inclusion under that prefix. The data supplied shall be adequate for the engineering staff to make a determination as to whether or not the proposed segment is to be included.			
3.2.2.1.6-13	The system segment registration process shall allow users to view the unique 6-letter segment prefix codes already in use.			
3.2.2.1.6-14	The system shall provide a web interface for developers to review the Socket/UID/GID data and request reservation of IDs for their use.			
3.2.2.1.6-15	The system shall send a flag/alert to the DII COE Engineering Office within 48 hours of a new prefix/segment name being registered.			
3.2.2.1.6-16	The system segment registration process shall include a mechanism for the engineering staff to approve/disapprove any proposed segment.			
3.2.2.1.6-17	The system shall set flag in the MIS for new prefix/segment names that have been registered to indicate that manual review of the name is required prior to approval of the assigned name.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.6-18	The segment catalog shall include the following information for each registered segment and application: a. Segment name b. Segment prefix c. Segment directory name d. Segment type (software, data, DII COE component, COTS, account group, database, or patch) e. System resources (e.g., port assignments, UIDs requested, Remote Procedure Call (RPC) address requested) f. Estimated memory required by the segment g. Estimated disk storage requirements h. List of boot and background processes i. Releasability restrictions (especially export restrictions) j. Platform availability k. Short paragraph describing the segment features unclassified picture of the segment's user interface (Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), or X11 Bitmap format) l. Authorization keys (assigned by DISA) m. List of related segments n. List of keywords for use in catalog searches o. Program Management Point-of-Contact p. Technical Point-of-Contact q. Process Point-of-Contact.			

3.2.2.1.7 Test Readiness Review Requirements

TBD

3.2.2.1.8 Inventory Support Requirements

DII COE system inventory support requirements for CM Services software are provided in Table 3.2.2.1.8-1.

Table 3.2.2.1.8-1. DII COE System Inventory Support Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.8-1	DII COE CM tools shall support site hardware and software inventory activities.			
3.2.2.1.8-2	The system shall maintain a repository of data on current deployed DII COE system hardware CIs.			
3.2.2.1.8-3	The system shall enable a user to update (add, modify, delete) data on current deployed DII COE system hardware CIs.			
3.2.2.1.8-4	The system shall be able to maintain an inventory of DII COE hardware and software CIs for a site.			
3.2.2.1.8-5	The system shall enable a user to update (add, modify, delete) DII COE system hardware and software CI inventory data.			
3.2.2.1.8-6	The system shall be able to perform automatic data collection for DII COE system hardware and software CI inventory data.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.8-7	The system shall enable the user to produce formatted reports containing CI software signature data collected on a DII COE system and output those reports for display or printing.			

3.2.2.1.9 Schedule Calendar Requirements

Schedule Calendar requirements for CM Services software are provided in Table 3.2.2.1.9-1.

Table 3.2.2.1.9-1. Schedule Calendar Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.9-1	Support for DII COE scheduling shall be provided.			
3.2.2.1.9-2	DII COE scheduling shall include the timeframe for requirements gathering, submission, and documentation.			
3.2.2.1.9-3	DII COE scheduling shall include the coordination timeframe for requirements solution identification (when requirement solution needed).			
3.2.2.1.9-4	DII COE scheduling shall include the development timeframe for requirements solution implementation.			
3.2.2.1.9-5	DII COE scheduling shall include the testing and integration timeframe for requirements implementation into the DII COE.			
3.2.2.1.9-6	DII COE scheduling shall include the distribution timeframe for DII COE releases.			
3.2.2.1.9-7	DII COE scheduling shall include the timeframes for meetings of DII COE Management Boards, Groups, and Subpanels.			
3.2.2.1.9-8	DII COE scheduling shall include the identification of resources necessary to manage the scheduling process.			
3.2.2.1.9-9	As appropriate, DII COE scheduling shall be deconflicted and approved by the applicable DII COE Management Board, Group, or Subpanel.			
3.2.2.1.9-10	As appropriate, DII COE scheduling shall include the reevaluation of the necessary resources allocated to manage the scheduling processes.			
3.2.2.1.9-11	The system shall provide the capability for authorized users to create, update, modify, and post on the web the Segment Delivery Calendar.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.9-12	The system shall provide the capability for authorized users to create, update, modify, and post on the web a CM Milestone Event Schedule. For each event shown on the schedule, the system shall track and maintain a historical record of changes for the following information: a. Event priority b. Event criticality to accomplishment of CM objectives c. Event planned start date d. Event planned end date e. Event actual start date f. Event actual end date d. Reason(s) for schedule changes e. Event completion status (expressed as a percentage, if applicable) f. Event dependencies g. Organization/ Point-of-Contact responsible for coordination and completion of the event h. Event schedule thresholds i. Activities, programs, releases, etc., impacted by changes to event schedule j. Overall impact of changes to event schedule.			

3.2.2.1.10 Electronic Submission and Acceptance Requirements

Electronic submission and acceptance requirements for CM Services software are provided in Table 3.2.2.1.10-1.

Table 3.2.2.1.10-1. Electronic Submission Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.10-1	DAD shall support the capability to electronically submit assets to DAD for processing by the appropriate organization (e.g., Configuration Management, or Testing).			
3.2.2.1.10-2	The system's Delivery and Scheduling System shall provide the capability for authorized users to designated whether a segment planned for delivery is classified or unclassified.			
3.2.2.1.10-3	The system shall be able to track and support queries on which segments scheduled for delivery are classified and which, if any, of the required documentation accompanying classified segments will be classified.			
3.2.2.1.10-4	The system shall be able to store, update and support queries on Delivery Checklist information for delivered segments.			
3.2.2.1.10-5	The system shall be able to track and support queries on information provided in the Delivery Letters that accompany segment deliveries.			
3.2.2.1.10-6	The system shall provide the capability for developers to compress and encrypt segments for electronic submission across the Internet.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.10-7	The system shall provide the capability to accept electronic submissions of DII COE segment Delivery Letters, Delivery Checklists, and Segment Release Bulletins. The system shall support and manage electronic submissions received over the Internet, through web-based interfaces, and through other electronic media, such as tapes.			
3.2.2.1.10-8	The system shall provide the capability for decompressing compressed segments.			
3.2.2.1.10-9	The system shall provide the capability to convert segments to raw files that can be scanned. This capability shall convert the segment to a sub-directory with all the segment's files. The sub-directory name shall be that of the segment.			
3.2.2.1.10-10	The system shall provide the capability for authorized users to build scripts (UNIX) to facilitate electronic submission and acceptance procedures.			

3.2.2.1.11 Electronic Acceptance Requirements

Electronic acceptance requirements for CM Services software are provided in Table 3.2.2.1.11-1.

Table 3.2.2.1.11-1. Electronic Acceptance Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.11-1	The system shall provide an automated segment verification utility for submitted segments. The segment verification utility shall verify/record segment name, version, prefix, external segment requirements and requirements and references to COTS products. The segment verification utility shall decompile and scan all segments for key words that indicate a licensed COTS product and determine license requirements for that segment.			
3.2.2.1.11-2	Delivered DII segments shall incorporate a fixed file/directory structure as defined in Chapter 5 of the I&RTS.			
3.2.2.1.11-3	The system shall provide the capability to detect and record segment dependency information ("REQUIRES" summary area) from the segment raw files created from the tape.			
3.2.2.1.11-4	For each segment delivered, the system shall be able to identify segment documentation for which a hard copy is required. (See Table 3.2.2.1.11-2 for a listing of which hard copy documents are required).			
3.2.2.1.11-5	The system shall provide the capability to identify and track the delivery and status of DII COE Kernel Platform Certification documentation required for segments being delivered under the auspices of the DII COE Kernel Platform Certification Program by developers. The required documentation is identified in the current version of the *DII COE Kernel Platform Certification Program* document.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.11-6	The system shall provide the capability to identify valid, current documentation waivers for segments being delivered by developers.			
3.2.2.1.11-7	The system shall be able to determine which, if any, of the following documents are covered by the documentation waiver for a specific segment: a. Software Version Description (SVD) b. Installation Procedures (IP) c. System Administrator's Manual (SAM) [1] d. User's Manual (UM)[1] e. Programmer's Manual (PM) [1] f. Application Program Interface Reference Manual (APIRM)[1] g. Software Product Specification (SPS)[2] h. Database Design Document (DBDD)[3] i. Software Test Plan (STP) j. Software Test Description (STD) k. Software Test Report (STR) l. Software Design Description (SDD)[2] m. Interface Design Document (IDD) [2] n. Errata Sheet (ES) [2]			
3.2.2.1.11-8	The system shall be able to store and support queries on existing documentation waivers for delivered segments.			
3.2.2.1.11-9	The system shall be able to track and support queries on export and release restrictions associated with segment documentation.			
3.2.2.1.11-10	The system shall provide the capability to display the contents of the segment's files.			
3.2.2.1.11-11	The system shall provide the capability to compare the segment information provided on a submitted tape with the information provided when the segment was originally registered.			
3.2.2.1.11-12	The system shall provide the capability to report on any discrepancies detected when comparing the segment information provided on a submitted tape with the information provided when the segment was originally registered, including the segment version, name, prefix, dependencies, etc.			
3.2.2.1.11-13	The system shall provide the capability to identify and report on fixes and changes that have been approved for incorporation into submitted segments and documentation.			
3.2.2.1.11-14	The system shall provide the capability for authorized users to selectively store each individual segment from a multi-segment tape to a disk.			

[1] If the segment being delivered is a COTS product, then the developer must deliver a copy of the manufacturer's documentation which provides the equivalent information.

[2] At Government Request. This document is to be delivered at the request of the cognizant Chief Engineer.

[3] Required if the segment being delivered is a database segment.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.11-15	The system shall provide the capability for authorized users to copy the table of contents from a submitted segment tape to disk and alphabetically sort the segments listed.			
3.2.2.1.11-16	Segment loading and parsing functions shall be supported for both Solaris and HP operating systems.			
3.2.2.1.11-17	The system shall provide the capability for authorized users to store segment information extracted from submitted tapes into the appropriate records in the MIS database.			

Table 3.2.2.1.11-2. Printed (Hard Copy) Requirement

Document	**DII COE**	**GCCS**
Delivery Letter	Required	Required
Delivery Checklist	Required	Required
Installation Procedures (IP) *(DII COE Only)*	Required	
Software Version Description (SVD)	Required	Required
System Administrator's Manual (SAM)	Note 1	Note 1
User's Manual (UM)	Note 1	Note 1
Software Product Specification (SPS)	Note 1	Note 1
Database Design Document (DBDD)	Note 1	Note 1
Software Test Plan (STP)	Note 1	Note 1
Software Test Description (STD)	Note 1	Note 1
Software Test Report (STR)	Note 1	Note 1
Application Program Interface Reference Manual (APIRM)	Note 1	Note 1
Programmer's Manual	Note 1	Note 1
Software Design Description (SDD)	Note 1	Note 1
Interface Design Document (IDD)	Note 1	Note 1
Errata Sheet (ES)	Note 1	Note 1
GCCS Segment Release Bulletin (SRB) *(GCCS Only)*		Required
DII COE Kernel Platform Certification Application Form *(KPC Only)*	Required	
Government Supplied Kernel Software (GSKS) Build Document *(KPC Only)*	Required	
Printout of the contents of the *SegName* and *Version* Descriptor Files	Required	Required
Intellectual Property Rights Agreement Attachment	Required	Required
Y2K Compliance Attachment *(GCCS Only)*	Note 1	Required

Note 1: A hard copy of these documents will only be required to be delivered if the cognizant Chief Engineer requests such. Otherwise, per guidance given at the critical design reviews, soft copies are sufficient.

3.2.2.1.12 Configuration Identification and Selection Metrics Requirements

The requirements covered by this section address metrics designed to measure the efficiency and accuracy of established configuration identification processes. Configuration identification and selection metrics requirements for CM Services software are provided in Table 3.2.2.1.12-1. (See also Appendix B for an overview of metrics management approach.)

Table 3.2.2.1.12-1. Configuration Identification and Selection Metrics Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.12-1	DII COE Configuration Management shall include the identification of potential problem areas within the DII COE development and management processes.			
3.2.2.1.12-2	Metrics shall be identified with which to classify, verify, and validate problem areas.			
3.2.2.1.12-3	Potential solutions to manage problem areas shall be identified to capture, analyze and report on the problem areas.			
3.2.2.1.12-4	As appropriate, resources shall be allocated to implement problem area solutions.			
3.2.2.1.12-5	Metrics to evaluate problem area solutions shall be developed to measure the effectiveness of the solutions.			
3.2.2.1.12-6	As appropriate, reallocation of resources shall occur to help support problem area solutions.			
3.2.2.1.12-7	The system shall provide the capability for authorized users to generate Gantt Charts and graphs and formatted and ad hoc reports depicting information on Budgeted Costs and Actual Costs of work performed/scheduled as reported in each contractor's Cost and Schedule Status Report, or equivalent report.			
3.2.2.1.12-8	The system shall provide the capability to calculate, display and output the Earned Value (also known as Budgeted Cost of Work Performed (BCWP)) for each DII COE Release that shows the amount of work completed on the release. BCWP equals the percent of tasks completed multiplied by the planned cost for each task at the current time. [Project Control Panel Gauge #1]			
3.2.2.1.12-9	The system shall provide the capability to calculate, display and output the Actual Cost for each DII COE Release (also known as Actual Cost of Work Performed (ACWP)) for each DII COE Release that shows the cumulative cost incurred for the release to date using the actual cost of each task at the current time for the DII COE Release. [Project Control Panel Gauge #2]			
3.2.2.1.12-10	The system shall provide the capability to generate, display and output the Elapsed Time Gauge of the Project Control Panel that shows the end date for the current reporting period. For this gauge the system shall be able to display the Schedule At Completion (SAC) mark that shows the original scheduled completion date for the DII COE Release. [Project Control Panel Gauge #3]			
3.2.2.1.12-11	The system shall provide the capability to calculate the Cost Performance Index (CPI) for each DII COE Release and display CPI graphically and on a chart. CPI shall be determined by dividing Budgeted Cost of Work Performed by the cumulative Actual Cost of Work Performed (BCWP/ACWP). [Project Control Panel Gauge #4]			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.12-12	The system shall provide the capability to calculate the To-Complete Performance Index (TCPI) for each DII COE Release and display TCPI graphically and on a chart. TCPI shall be determined by dividing the work remaining for the DII COE Release (Total original budget for the release, known as Budget At Completion (BAC) minus BCWP) by the current estimate of remaining cost (Best estimate for the total cost of the release, known as Estimate At Completion (EAC) minus ACWP) expressed as ((BAC-BCWP)/(EAC-ACWP)). [Project Control Panel Gauge #5]			
3.2.2.1.12-13	The system shall provide the capability to calculate the Completion Efficiency (CE) for each DII COE Release and display CE graphically and on a chart. CE shall be determined by dividing BAC by EAC to estimate the productivity required to complete the release within a project total cost. [Project Control Panel Gauge #6]			
3.2.2.1.12-14	The system shall provide the capability to calculate the Monthly CPI for each DII COE Release and display Monthly CPI graphically and on a chart. Monthly CPI shall be determined by dividing Monthly Budget Cost of Work Performed by the Monthly Actual Cost of Work Performed (Monthly BCWP/Monthly ACWP). [Project Control Panel Gauge #6]			
3.2.2.1.12-15	The system shall provide the capability to generate, display and output the DII COE Release Total Program Performance Efficiency Chart that compares TCPI, CE, CPI and Monthly CPI over time. [Project Control Panel Gauge #6]			
3.2.2.1.12-16	The system shall be able to determine the Total Due indicator of the Quality Gate Task Status for the current month/reporting period. Total Due shall be calculated as the total number of tasks scheduled for completion during the current reporting period/month plus any overdue tasks from previous periods. Total Due indicates the total quantity of work required for the project to keep pace with the release schedule. [Project Control Panel Gauge #7]			
3.2.2.1.12-17	The system shall be able to determine the Completed On Time indicator of the Quality Gate Task Status for the current month /reporting period. Completed On Time shall be calculated as the total number of tasks originally scheduled for completion during the current reporting period/month that were completed by their original scheduled due date. Completed On Time indicates how well the release effort is keeping up with scheduled work. [Project Control Panel Gauge #7]			
3.2.2.1.12-18	The system shall be able to determine the Completed Late indicator of the Quality Gate Task Status for the current month/reporting period. Completed Late shall be calculated as the total number of tasks completed late, as well as any overdue tasks from previous periods/months that were completed in this period. Completed Late indicates how well the release effort is completing work, even if it is late according to the original schedule. [Project Control Panel Gauge #7]			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.12-19	The system shall be able to determine the Total Overdue indicator of the Quality Gate Task Status for the current month/reporting period. Total Overdue shall be calculated as the total number of tasks for all previous reporting periods that are overdue by the end of the current reporting period. Total Overdue is equal to Total Due minus Completed On Time and Completed Late. Total Overdue indicates the quantity of work needed to get the release back on schedule. [Project Control Panel Gauge #7]			
3.2.2.1.12-20	The system shall provide the capability to generate, display and output the Quality Gate Task Status for the current month/reporting period that shows the completion status of tasks during the current reporting period. The criterion used shall be a yes/no indicator that shows a task has been completed. The indicators to be displayed are Total Due, Completed On Time, Completed Late, and Total Overdue. [Project Control Panel Gauge #7]			
3.2.2.1.12-21	The system shall provide the capability to generate, display and output the Quality Gate Tasks Completed Graph that shows the cumulative number of tasks associated with a release completed by the end of each reporting period to date plotted with the cumulative number of tasks scheduled for completion. [Project Control Panel Gauge #8]			
3.2.2.1.12-22	The system shall provide the capability to generate, display and output the CM Churn Per Month Chart. The CM Churn Per Month shall be calculated by taking the number of baselined CIs that have been modified and re-checked into CM system over the last reporting period and dividing it by the total number of baselined CIs in the system at the end of the period. It is expressed as a percentage. [Project Control Panel Gauge #9]			
3.2.2.1.12-23	The system shall provide the capability to generate, display and output the Requirement Change Per Month Chart. The Requirement Change Per Month shall be calculated by dividing the number of new, changed or deleted requirements specified in this reporting period by the total number of requirements in the system at the end of the period. It is expressed as a percentage. [Project Control Panel Gauge #10]			
3.2.2.1.12-24	The system shall provide the capability to generate, display and output the Risk Exposure Chart that shows each identified risk to releases plotted by its cost consequence and probability. The probability shall be expressed in terms of occurrences over the life of the software release. [Program Control Panel Gauge #13]			
3.2.2.1.12-25	The system shall provide the capability to generate, display and output the Risk Reserve Chart for each release that shows the total risk exposure for cost and schedule compared to the current cost and time risk reserves for the release. Risk Exposure for a release risk shall be calculated by multiplying the probability by the consequence of that risk. A first approximation of the total cost risk exposure to the release can be made by summing the individual cost risk exposures for all risks. [Program Control Panel Gauge #14]			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.12-26	The system shall provide the capability to generate, display and output the Defects By Activity Chart that displays the number of detected defects in (1) requirements, (2) design, (3) code, and (4) test that are open and the number of defects closed in each phase of the project. Defects are problems that, if not removed, could cause a program to fail or produce incorrect results. Defects shall be prioritized by severity level, with those labeled as numeral 1 being the most serious. [Project Control Panel Gauge #16]			
3.2.2.1.12-27	The system shall provide the capability for authorized users to generate tabular formatted and ad hoc reports depicting event information tracked in the CM Milestone Event Schedule.			
3.2.2.1.12-28	The system shall provide the capability for authorized users to generate Gantt Charts and graphs depicting the differences between the original plan and subsequent changes in event data tracked in the CM Milestone Event Schedule.			
3.2.2.1.12-29	The system shall provide the capability to track, generate reports on, and graphically depict the following summary information on submitted segments: a. Number of segments submitted manually b. Number of segments submitted electronically c. Number of segments unsuccessfully submitted manually d. Number of segments unsuccessfully submitted electronically e. Number of segments submitted that were not pre-registered.			
3.2.2.1.12-30	The system shall provide the capability to track, generate reports on, and graphically depict the following information for each DII COE segment: a. How the segment is submitted (electronically or manually) b. Number of times a specific version/build of a segment is submitted unsuccessfully c. Segment size (MB).			
3.2.2.1.12-31	The system shall provide the capability to query Build Plan information; for example, which release/build plan will have specified capabilities.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.12-32	The system shall provide the capability to track, generate reports on, and graphically depict the following information for each CSCI: a. Software requirement discrepancy status (cumulative total of requirements linked to the CSCI and cumulative total number of requirements resolved) b. Total number of software lines of code (SLOC) c. Total number of SRS requirements linked to the CSCI d. Number of SRS requirements added due to approved ECPs e. Number of SRS requirements modified due to approved ECPs f. Number of SRS requirements deleted due to approved ECPs g. Number of SLOC affected by approved ECPs.			
3.2.2.1.12-33	The system shall provide the capability to track, generate reports on, and graphically depict the following summary information on COTS licenses: a. Number of segments requiring COTS licenses b. Number of segments that require each individual COTS license c. Number of copies of each COTS license purchased for a specific DII COE software release (including follow-on procurements to meet customer requests) d. Number of licenses for a specific COTS product that are used/unused for a specific DII COE software release e. The number of licenses distributed to each DII COE customer and Service/Agency Point-of-Contact f. Number of copies of a specific COTS license that were requested after all licenses had been distributed g. Number of requests for a specific COTS license that were unfilled at the time of the request h. Number of copies of a specific COTS license that had to be ordered after the original COTS license purchase to fill customer requests.			
3.2.2.1.12-34	The system shall be able to generate and display graphs and tables depicting the number of requirements linked to specific DII COE capabilities and CSCIs. This information indicates the criticality of system capabilities/CSCIs.			
3.2.2.1.12-35	The system shall provide the capability for authorized users to generate Gantt Charts and graphs depicting summary and statistical information on the following: a. the number of new requirements (by time period), b. the number of approved and disapproved requirements (by time period) c. the number of unfinanced and financed requirements (by time period) d. the number of requirements satisfied and closed in DII COE Build Plans and Releases (by time period) e. requirement cost to implement (by requirement priority and level of effort) f. requirement priority g. requirement originators.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.12-36	The system shall provide the capability for authorized users to generate Gantt Charts and graphs depicting summary and statistical information on the percentage of approved/validated requirements linked to each of the following technical documents, as appropriate: (1) MNS (2) ORD (3) UFD (4) OCD (5) SSS (6) IRS (7) SRS (8) SDD (9) IDD (10) DBDD (11) SPS (12) ECP.			
3.2.2.1.12-37	The system shall provide the capability for authorized users to generate Gantt Charts and graphs depicting summary and statistical information on the percentage of approved/validated requirements linked to each of the following test documents, as appropriate: a. TEMP/TEP b. DTP c. STP d. STD e. SDF.			
3.2.2.1.12-38	The system shall provide the capability to track the number of changes made to each DII COE requirement being tracked by the system.			
3.2.2.1.12-39	The system shall provide the capability to track and report on the amount of time required for new requirement processing tasks according to requirement priority and level of effort to implement, to include the following: a. From receipt of requirement to requirement validation or disapproval/closure by TWG b. From requirement validation to requirement approval/disapproval by DII COE Engineering Office c. From requirement approval by Engineering to requirement assignment to a build plan d. From requirement approval by Engineering to requirement inclusion in ECP/SCN or SCP, as appropriate e. From requirement assignment to a build plan to its implementation in software (per developer) and closure. f. From requirement inclusion in SCN to release of updated technical documentation citing new/modified requirement.			

3.2.2.2 Configuration Control Requirements

3.2.2.2.1 Release Control Panel Requirements

Release control panel requirements for CM Services software are provided in Table 3.2.2.2.1-1.

Table 3.2.2.2.1-1. Release Control Panel Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.1-1	The system shall provide the ability to generate, monitor and maintain Milestone schedules for each scheduled release, including the status and schedule of sub-projects in each release. Modifications to the schedule shall require the entry of an explanation for the schedule change as well as any known schedule impacts the change will have.			
3.2.2.2.1-2	The system shall provide scheduling capabilities, including the ability to baseline schedules and track schedule changes. Scheduling capabilities shall be linked to other CM Services tools and applications.			
3.2.2.2.1-3	The system shall provide the ability to generate, monitor and maintain the current schedules of segments going through integration and testing. Modifications to the schedule shall require the entry of an explanation for the schedule change as well as any known schedule impacts the change will have. If delays result from segment dependencies, each dependency causing the delay should be explicitly noted.			
3.2.2.2.1-4	System scheduling capabilities shall include the ability to track and record which scheduled activities are delayed or otherwise modified in the schedule.			
3.2.2.2.1-5	The system shall be able to provide the current status of all segments associated with each planned/ scheduled DII COE-based system release.			
3.2.2.2.1-6	System scheduling capabilities shall include the ability to show the expected beginning and end date of the Pre-Production effort defining a specific release's Pre-Production Reporting Period. The timeline shall be determined based on the analysis of metrics associated with the build list. The reporting period element will be able to access a history log of previous begin/end dates and reasons for any changes. Pre-Production activities to be tracked, at a minimum, shall include: product delivery acceptance, testing, integration, product assurance, packaging, distribution, fielding and initial operations. A mechanism shall be included for tracking actions items and new directions from meetings that impact the Pre-Production schedule.			
3.2.2.2.1-7	System scheduling capabilities shall include the ability to show elapsed Pre-Production time once Pre-Production efforts have started for a particular release.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.1-8	Pre-Production scheduling capabilities shall include the ability to report the following information on scheduled tasks: a. Task dependencies b. Task assumptions c. Total tasks currently due d. Tasks completed on time according to schedule e. Tasks completed late according to schedule f. Total tasks currently overdue according to schedule			
3.2.2.2.1-9	Pre-Production scheduling capabilities shall include the ability to generate a graphical representation of task completion over time (planned vs. actual) to see where spikes occur and monitor rate of completion.			
3.2.2.2.1-10	The system shall track and maintain information on the quality of the released product. The system shall be able to track and quantify (# of defects and estimate dollar value associated with cost to fix once fielded) the impact of defects found by Pre-Production activity: Segment Acceptance/Delivery, DII COE Compliance Checks, Basic Security Checks, Configuration/Performance Checks, Documentation Reviews, Functional Testing, Preparing Distribution Media, System Build/Install, Training, Fielding, and Operations.			
3.2.2.2.1-11	The system shall track warnings received (by e-mail. suggestion box, etc.) about some portion of the Pre-Production process.			
3.2.2.2.1-12	The system shall track and maintain information on the risks associated with Pre-Production efforts. Key risk elements shall be quantified with respect to the probability of occurrence and the cost or consequences of the occurrence. The drop down detail shall provide a formal statement of the risk (including originator, date identified, source/ classification of risk, probability, priority, impact, and a timeframe), and indicate mitigating strategy/steps employed, results expected (along with a contingency plan, trigger, and authorization), and a Point-of-Contact for tracking. The risk shall be closed out once the window for opportunity has passed or probability has dropped below 5%.			
3.2.2.2.1-13	The system shall maintain a “Risk Reserve” indicator that shows the status of the Pre-Production risk posture (reserve vs. exposure) with respect to funding and schedule.			
3.2.2.2.1-14	The system shall track and provide reports on risk status. The risk status reports shall include the following: a. Top 10 risk items b. Unresolved risk items on the critical path c. The number of risk items resolved to date d. New risk items since last report e. Unresolved risk items f. The probable cost for unresolved risk vs. risk reserve.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.1-15	The system shall provide the ability to generate, monitor and maintain software release/deployment schedules of DII COE-based systems going to each Service and Agency Point-of-Contact for distribution and to GCCS sites. Modifications to the schedule shall require the entry of an explanation for the schedule change.			
3.2.2.2.1-16	In support of segment release control, the system shall record data and/or metrics pertinent to the following items: a. high-level progress identification b. productivity c. completion d. change (requirements/interfaces/schedule) e. defects spotted by activity/quality gate f. risk			
3.2.2.2.1-17	The system shall be able to track and maintain software "Earned Operational Utility". The "Earned Operational Utility" element shows the cumulative operational earned utility provided by the segments and associated applications that have passed testing and integration efforts. Each segment's operational utility is estimated based on the number and criticality of applications that depend on that segment for operation. This capability also requires a drop down into a breakout of what segments are needed to run each application and the associated "operational utility" of each associated segment.			
3.2.2.2.1-18	The system shall identify the functional capabilities to be provided in each DII COE-based system release, including new capabilities due to engineering changes and system modifications.			
3.2.2.2.1-19	The system shall be able to generate and output printed reports containing all GSPR information from Release Control Panels to include but not limited to: a. Quality Information (# of open/closed defects found by activity) b. Interface changes c. Requirements and schedule changes d. Risk impacts e. Productivity information per release efforts f. High-level progress g. Completion status (on-time, late, out-standing)			
3.2.2.2.1-20	The system shall provide financial budget and cost tracking capabilities. The system shall be able to generate the total amount budgeted and spent (cumulative) for each previous release as well as current release efforts. This includes costs for any follow-on fixes (e.g., GSPRs) or calls for assistance from the field. This capability also requires a drop down menu that breaks out cost by categories: Labor vs. equipment, licenses, supplies, building lease, phone/communication bills, and travel; also requires a breakout between contract vs. Government components.			
3.2.2.2.1-21	The system shall maintain a list of DII COE user organizations, listing the organization names, phone numbers, offices, responsibilities and expectations.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.1-22	The system shall maintain a list of DII COE-based system customers, listing the customer names, phone numbers, offices, responsibilities and expectations.			
3.2.2.2.1-23	The system shall be able to track and report on the effectiveness of staff resource allocation and whether staff resources are sufficient to complete the scheduled tasks.			
3.2.2.2.1-24	The system shall be able to track and report on the planned level of effort, the actual level of effort, and the losses in staff measured by labor category. For each CSCI, labor category, and experience level tracked, the system shall record the following information: a. Labor category b. Experience level c. Number of personnel planned to be on staff for the reporting period d. Number of personnel actually on staff in the reporting period e. Number of unplanned losses in personnel that occurred f. Number of labor hours planned to be expended in the reporting period (cumulative) g. Number of labor hours actually expended in the reporting period (cumulative) h. Number of labor hours that were expended as overtime.			
3.2.2.2.1-25	The system shall provide the capability for authorized users to generate formatted and ad hoc reports, charts, and graphs comparing planned and actual levels of effort and personnel.			
3.2.2.2.1-26	The system shall provide the capability for authorized users to calculate, display and output the Voluntary Turnover Per Month. Voluntary Turnover Per Month is calculated by dividing the number of staff leaving during each reporting period by the number of staff at the beginning of the reporting period. The result is to be expressed as a percentage. [Project Control Panel Gauge #11]			
3.2.2.2.1-27	The system shall provide the capability for authorized users to calculate, display and output the Overtime Per Month. Overtime Per Month is calculated by dividing the overtime hours by the base working hours for all project staff in the reporting period. The result is to be expressed as a percentage. [Project Control Panel Gauge #12]			

Additional requirements associated with the Release Control Panel are addressed under Configuration Control Metrics in Paragraph 3.2.2.2.15.

In addition to the above requirements, the CMIS SRS specified that Control Panels need the following functionality (with WEB based access to authorized users) with drill down capability down into the MIS for details:

a. High-level progress identification

1. Earned utility (cumulative versus Total budgeted per release) as identified by Joint Staff during the requirement/fixes prioritization with operational impact qualifiers.
2. Months (cumulative versus Total budgeted per release)
3. Funding (cumulative versus Total budgeted per release)

b. Productivity

1. Processes completed versus Cost expended per release
2. Efficiency over time per release

c. Completion

1. Tasks completed per release
2. Quality gate progress/status

d. Change

1. Requirements
2. Interfaces
3. Schedule

e. Defects found

1. Delivery
2. Integration
3. Configuration build test
4. Segment test
5. Low-bandwidth testing
6. Multi-node testing
7. Packaging for distribution
8. Site installation
9. Field reports

f. Risks

1. Identifiable risks, impact, and probability
2. Mitigation plans and status
3. Liability (time and funding
4. Risk reserves: Available versus Expended
5. Anonymous risk alert/resolution

3.2.2.2.2 Scheduling Requirements

Scheduling requirements for CM Services software ar e provided in Table 3.2.2.2.2-1.

Table 3.2.2.2.2-1. Scheduling Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.2-1	The system shall provide the capability for authorized users to create, update, modify, and post on the web a Segment Processing Schedule. For each segment the schedule shall track the following events: a. Segment Development b. DII COE/GCCE Engineering Segment Review c. Successful Segment Delivery d. Segment Integration & Test e. Segment Quality Assurance (QA) Test f. Segment Functional Test g. Segment Status Review h. Segment Approval for Release			
3.2.2.2.2-2	For each event for each segment shown on the Segment Processing Schedule, the system shall track and maintain a historical record of changes for the following information: a. Event planned start date b. Event planned end date c. Event actual start date d. Event actual end date e. Reason(s) for schedule changes f. Event completion status (expressed as a percentage, if applicable) g. Organization/ Point-of-Contact responsible for coordination and completion of the event.			
3.2.2.2.2-3	DII COE development, testing, integration, and production schedules shall be updated as appropriate.			
3.2.2.2.2-4	Schedules shall be deconflicted and authorized by the cognizant approval organization.			
3.2.2.2.2-5	As appropriate from schedule deconfliction, resources allocated to schedules shall be reevaluated and modified as required.			
3.2.2.2.2-6	The system shall be able to verify receipt of documentation and CIs.			
3.2.2.2.2-7	The system shall provide the capability to generate reports on documentation and CIs that have been received during a specified time period and that meet specified criteria.			
3.2.2.2.2-8	The system shall be able to generate and output the PCCB agenda.			

3.2.2.2.3 DII Asset Distribution (DAD) Requirements

The CM Services software shall provide capabilities for electronic distribution of COE assets both internally on a local network and externally using wide area networks. DII Electronic assets include software segments, software patches, database segments, related tools, documentation, and associated software licenses of the DII Asset Programs. These programs include: COE, GCCS, GCSS, Defense Message System (DMS), Defense Enterprise Licensing

(DEL), Shared Data Environment (SHADE), and Information Security (INFOSEC). The services provided by DAD processes shall include: ordering systems, access to documentation, access to CIs, and database tracking of what has been received by the users.

DAD will be used by and within US DoD Services and Agencies and any other authorized organizations. DAD users will include Defense software developers, and Service and Agency personnel.

Currently, segment delivery is being done manually, v ia copying tapes and documents with some downloading off of the Internet. The automated asset distribution and tracking processes are under development and are also addressed in the DII Asset Distribution Sub-Panel SRS. The DAD products will be segments, forms for allowing users to receive segments and a tracking mechanism to allow DISA and Services visibility into configurations at users sites. Information collected on asset distributions will be used by planning, license management and installation teams. DAD specified and implied functional requirements are addressed in the following paragraphs.

3.2.2.2.3.1 DAD Browse and Search Requirements

DAD browse and search requirements for CM Services software are provided in Table 3.2.2.2.3.1-1.

Table 3.2.2.2.3.1-1. DAD Browse and Search Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.3.1-1	DAD shall provide the capability to browse for assets.			
3.2.2.2.3.1-2	DAD shall provide the capability to search for assets.			
3.2.2.2.3.1-2.1	DAD shall provide the capability to conduct natural language searches.			
3.2.2.2.3.1-2.1.1	DAD shall provide the capability to conduct pattern (wildcard) searches.			
3.2.2.2.3.1-2.2	DAD shall provide the capability to conduct searches by specifying search criteria in any one attribute or in any combination of attributes within a Library. Attributes are identified in the Internal Data Requirements section.			
3.2.2.2.3.1-3	DAD shall provide the capability to sort presentation of browse or search asset list by user-selected attribute.			
3.2.2.2.3.1-4	DAD shall provide the capability to view the metadata of any selected asset.			

3.2.2.2.3.2 User-Initiated Download and Subscription Requirements

DAD user-initiated download and subscription requirements for CM Services software are provided in Table 3.2.2.2.3.2-1.

Table 3.2.2.2.3.2-1. User-Initiated Download and Subscription Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.3.2-1	DAD shall provide the capabilities to select and download assets.			
3.2.2.2.3.2-1.1	DAD shall show the results of search in a results list from which assets may be selected and downloaded.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.3.2-1.2	DAD shall allow selection and downloading of assets from a browse list.			
3.2.2.2.3.2-2	DAD shall provide the capability for users to select multiple assets and designate them as one download package.			
3.2.2.2.3.2-3	DAD shall provide the capability for users to make selections then download all selected assets with one download command.			
3.2.2.2.3.2-4	DAD shall provide the capability for users to schedule the download of assets at a time of their choice.			
3.2.2.2.3.2-5	DAD shall support the capability of monitoring the status of the download session.			
3.2.2.2.3.2-5.1	DAD shall show the user incremental download progress.			
3.2.2.2.3.2-5.2	DAD shall verify the accuracy of the completed download.			
3.2.2.2.3.2-6	DAD shall have the capability for the user to specify distribution of a selected asset or group of assets by 4mm tape, 8mm tape, or CD-ROM.			
3.2.2.2.3.2-7	DAD shall display the success or failure of the completed download, on an asset by asset basis.			
3.2.2.2.3.2-8	DAD shall provide the capability for users to subscribe to assets for later automatic delivery.			
3.2.2.2.3.2-9	DAD shall provide the capability for users to subscribe to information about assets, including asset availability.			

3.2.2.2.3.3 DAD Administration Requirements

DAD administration requirements for CM Services software are provided in Table 3.2.2.2.3.3-1.

Table 3.2.2.2.3.3-1. DAD Administration Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.3.3-1.1	DAD shall provide the capability to manage user groups.			
3.2.2.2.3.3-1.1.1	DAD shall provide the capability to create groups.			
3.2.2.2.3.3-1.1.2	DAD shall provide the capability to modify groups.			
3.2.2.2.3.3-1.1.3	DAD shall provide the capability to delete groups.			
3.2.2.2.3.3-1.1.4	DAD shall provide the capability to add users to groups.			
3.2.2.2.3.3-1.1.5	DAD shall provide the capability to delete users from groups.			
3.2.2.2.3.3-1.1.6	DAD shall provide the capability to produce reports listing available groups.			
3.2.2.2.3.3-1.1.7	DAD shall provide the capability to produce reports listing users by group.			
3.2.2.2.3.3-1.2	DAD shall provide the capability to manage asset groups.			
3.2.2.2.3.3-1.2.1	DAD shall provide the capability to create asset groups.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.3.3-1.2.2	DAD shall provide the capability to modify asset groups.			
3.2.2.2.3.3-1.2.3	DAD shall provide the capability to delete asset groups.			
3.2.2.2.3.3-1.2.4	DAD shall provide the capability to add assets to asset groups.			
3.2.2.2.3.3-1.2.5	DAD shall provide the capability to delete assets from asset groups.			
3.2.2.2.3.3-1.2.6	DAD shall provide the capability to produce reports listing available asset groups.			
3.2.2.2.3.3-1.2.7	DAD shall provide the capability to produce reports listing assets by asset groups.			
3.2.2.2.3.3-1.3	DAD shall provide the capability to limit access to specific asset groups to specific user groups.			
3.2.2.2.3.3-1.3.1	DAD shall provide the capability to specify specific asset groups as view-only, for specific user groups.			
3.2.2.2.3.3-1.3.2	DAD shall provide the capability to specify specific asset groups as view and download, for specific user groups.			
3.2.2.2.3.3-1.4	DAD shall provide the capability to select from which server or distribution site any one or more assets can be downloaded			
3.2.2.2.3.3-1.5	DAD shall provide the capability to divert a download request to a manual distribution process based on established criteria.			
3.2.2.2.3.3-1.5.1	DAD shall provide the capability to specify a file size limit for assets that can be downloaded.			
3.2.2.2.3.3-1.5.2	DAD shall provide the capability to specify asset licensing criteria for assets that can be downloaded.			
3.2.2.2.3.3-1.6	DAD shall provide the capability to manage asset metadata.			
3.2.2.2.3.3-1.6.1	DAD shall provide the capability to create asset metadata.			
3.2.2.2.3.3-1.6.2	DAD shall provide the capability to modify asset metadata.			
3.2.2.2.3.3-1.6.3	DAD shall provide the capability to delete asset metadata.			
3.2.2.2.3.3-1.7	DAD shall provide the capability to manage asset files.			
3.2.2.2.3.3-1.7.1	DAD shall provide the capability to add asset files.			
3.2.2.2.3.3-1.7.2	DAD shall provide the capability to delete asset files.			
3.2.2.2.3.3-1.8	DAD shall provide the capability to manage relationships between assets.			
3.2.2.2.3.3-1.8.1	DAD shall provide the capability to identify assets that are unchanged from previous system releases.			
3.2.2.2.3.3-1.9	DAD shall provide the capability to assign one asset to multiple asset groups.			
3.2.2.2.3.3-1.10	DAD shall provide the capability to package assets into groups for delivery.			
3.2.2.2.3.3-1.11	DAD shall provide the capability to schedule automatic delivery of multiple specified assets to multiple specified users.			
3.2.2.2.3.3-1.12	DAD shall provide the capability to initiate delivery of multiple specified assets to multiple specified users.			
3.2.2.2.3.3-1.13	DAD shall provide the capability to manage distribution tiers.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.3.3-1.14	DAD shall provide the capability to modify the content of all forms used to interact with users of a specific Library.			
3.2.2.2.3.3-1.14.1	DAD shall provide default content for all forms used to interact with user.			
3.2.2.2.3.3-1.14.2	DAD shall provide the capability to select default content to replace any customized content.			
3.2.2.2.3.3-1.14.3	DAD shall provide the capability to save custom content to use instead of default content.			
3.2.2.2.3.3-1.15	DAD shall provide the capability to deliver information to all users or subset of users.			
3.2.2.2.3.3-1.15.1	DAD shall provide the capability to notify users of availability of new asset(s) within a Library.			
3.2.2.2.3.3-1.15.2	DAD shall provide the capability to notify users of new complete releases (e.g., DII COE 3.4, or GCCS 3.0) within a Library.			
3.2.2.2.3.3-1.15.3	DAD shall provide the capability to notify users of expected delivery schedules.			
3.2.2.2.3.3-1.15.4	DAD shall provide the capability to notify users of any changes to asset(s) within a Library.			
3.2.2.2.3.3-1.15.5	DAD shall provide the capability to notify DAD administrators and users of forthcoming changes to a Library.			
3.2.2.2.3.3-1.15.6	DAD shall provide the capability to notify users of forthcoming changes to DAD.			
3.2.2.2.3.3-1.16	DAD shall have the capability to generate reports on current library instance status.			
3.2.2.2.3.3-1.16.1	DAD shall have the capability to generate reports on assets by collections.			
3.2.2.2.3.3-1.16.2	DAD shall have the capability to generate reports on assets by classes.			
3.2.2.2.3.3-1.16.3	DAD shall have the capability to generate reports on collection definition.			
3.2.2.2.3.3-1.16.4	DAD shall have the capability to generate reports on class definition.			
3.2.2.2.3.3-1.16.5	DAD shall have the capability to generate reports listing all assets by class or by collection.			
3.2.2.2.3.3-1.16.5.1	DAD shall have the capability to generate reports listing entire catalog (all assets) by class.			
3.2.2.2.3.3-1.16.5.2	DAD shall have the capability to generate reports listing entire catalog (all assets) by collection.			
3.2.2.2.3.3-1.17	DAD shall have the capability to generate reports on library instance usage analysis.			
3.2.2.2.3.3-1.17.1	DAD shall have the capability to generate reports on number of accesses by account privilege set (i.e., the roles of user, master administrator, library manager, account manager).			
3.2.2.2.3.3-1.17.2	DAD shall have the capability to generate reports on number of accesses of asset metadata.			
3.2.2.2.3.3-1.17.3	DAD shall have the capability to generate reports showing specific asset extractions and attempts for a Library over day, month, and year by user, user group, user's organization, asset, and user location, and download-success.			
3.2.2.2.3.3-1.17.4	DAD shall have the capability to generate reports showing asset extraction totals for a Library over day, month, and year by user, user group, user's organization, asset, and user location, and download-success.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.3.3-2.1	DAD shall provide the capabilities to manage user accounts.			
3.2.2.2.3.3-2.1.1	DAD shall provide the capabilities to add a user account.			
3.2.2.2.3.3-2.1.2	DAD shall provide the capabilities to modify a user account.			
3.2.2.2.3.3-2.1.3	DAD shall provide the capabilities to delete a user account.			
3.2.2.2.3.3-2.2	DAD shall deny access to any unauthorized users.			
3.2.2.2.3.3-2.3	DAD shall provide the capability for potential users to apply for accounts electronically.			
3.2.2.2.3.3-2.3.1	DAD shall provide the capability to specify the information desired on the Account Request form.			
3.2.2.2.3.3-2.3.2	DAD shall provide the capability for potential user to fill in the requested information on the Account Request.			
3.2.2.2.3.3-2.3.3	DAD shall provide the capability for the potential user to submit Account Request electronically.			
3.2.2.2.3.3-2.3.4	DAD shall provide the capability to automatically acknowledge receipt of Account Request.			
3.2.2.2.3.3-2.3.5	DAD shall provide the capability to review, accept, or reject Account Request electronically.			
3.2.2.2.3.3-2.3.6	DAD shall provide the capability to notify the requestor of acceptance or rejection of account request.			
3.2.2.2.3.3-2.4	DAD shall provide the capability to limit specific accounts to specific privileges.			
3.2.2.2.3.3-2.4.1	DAD shall limit privileges of an account to no more than the privileges of the account of the person granting the privileges.			
3.2.2.2.3.3-2.4.2	DAD shall provide the capability to manage specific privileges for each specific account.			
3.2.2.2.3.3-2.4.2.1	DAD shall provide the capability for an authorized account to add specific privileges for each specific account.			
3.2.2.2.3.3-2.4.2.2	DAD shall provide the capability for an authorized account to modify specific privileges for each specific account.			
3.2.2.2.3.3-2.4.2.3	DAD shall provide the capability for an authorized account to delete specific privileges for each specific account.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.3.3-2.4.2.4	DAD shall provide a list of choices for the following privileges: (1) User View/Download: View-Only, View and Download (2) Library Forms: Create, Modify, Delete, Default (3) Library Reports: Create, Modify, Delete (4) Asset Metadata: Create, Modify, Delete, Copy/Move (5) Collections: Create, Modify, Delete (6) Core Classes: Create, Modify, Delete (7) Core Attributes: Create, Modify, Delete (8) Classes: Create, Modify, Delete (9) Attributes: Create, Modify, Delete (10) Enumerations: Create, Modify/Delete (11) Synonyms: Create, Modify, Delete (12) Users: Create, Modify, Delete (13) Administrators: Create, Modify, Delete (14) User Groups: Create, Modify, Delete (15) Asset Groups: Create, Modify, Delete (16) Import/Export: Import, Export, Multiple Modify (17) Remote Sites: Create, Modify, Delete (18) Asset Files: Create, Delete			
3.2.2.2.3.3-2.4.3	DAD shall provide the capability to specify a default privilege set for other accounts. DAD shall provide default privilege sets for User, Master Administration, Library Management, and Account Management.			
3.2.2.2.3.3-2.4.3.1	DAD shall provide the capability to specify a default User privilege set including the following privileges: View/Download: View-Only (off), View and Download (on).			
3.2.2.2.3.3-2.4.3.2	DAD shall provide the capability to specify a default Master Administration privilege including the following privileges, except where the creating account does not have these privileges: (1) View/Download: View-Only (off), View and Download (on) (2) Library Forms: Create, Modify, Delete, Default (all on) (3) Library Reports: Create, Modify, Delete (all on) (4) Asset Metadata: Create, Modify, Delete, Copy/Move (all on) (5) Collections: Create, Modify, Delete (all on) (6) Core Classes: Create, Modify, Delete (all on) (7) Core Attributes: Create, Modify, Delete (all on) (8) Classes: Create, Modify, Delete (all on) (9) Attributes: Create, Modify, Delete (all on) (10) Enumerations: Create, Modify/Delete (all on) (11) Synonyms: Create, Modify, Delete (all on) (12) Users: Create, Modify, Delete (all on) (13) Administrators: Create, Modify, Delete (all on) (14) User Groups: Create, Modify, Delete (all on) (15) Asset Groups: Create, Modify, Delete (all on) (16) Import/Export: Import, Export, Multiple Modify (all on) (17) Remote Sites: Create, Modify, Delete (all on) (18) Asset Files: Create, Delete (all on)			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.3.3-2.4.3.3	DAD shall provide the capability to specify a default Library Management privilege set including the following privileges, except where the creating account does not have these privileges: (1) View/Download: View-Only (off), View and Download (on) (2) Library Forms: Create, Modify, Delete, Default (all on) (3) Library Reports: Create, Modify, Delete (all on) (4) Asset Metadata: Create, Modify, Delete, Copy/Move (all on) (5) Collections: Create, Modify, Delete (all on) (6) Core Classes: Create, Modify, Delete (all off) (7) Core Attributes: Create, Modify, Delete (all off) (8) Classes: Create, Modify, Delete (all on) (9) Attributes: Create, Modify, Delete (all on) (10) Enumerations: Create, Modify/Delete (all on) (11) Synonyms: Create, Modify, Delete (all on) (12) Users: Create, Modify, Delete (all on) (13) Administrators: Create, Modify, Delete (all on) (14) User Groups: Create, Modify, Delete (all on) (15) Asset Groups: Create, Modify, Delete (all on) (16) Import/Export: Import, Export, Multiple Modify (all on) (17) Remote Sites: Create, Modify, Delete (all off) (18) Asset Files: Create, Delete (all on)			
3.2.2.2.3.3-2.4.3.4	DAD shall provide the capability to specify a default Account Management privilege set including the following privileges, except where the creating account does not have these privileges: (1) View/Download: View-Only (off), View and Download (on) (2) Library Forms: Create, Modify, Delete, Default (all on) (3) Library Reports: Create, Modify, Delete (all on) (4) Users: Create, Modify, Delete (all on) (5) Administrators: Create, Modify, Delete (all off) (6) User Groups: Create, Modify, Delete (all on) (7) Asset Groups: Create, Modify, Delete (all off)			
3.2.2.2.3.3-2.4.4	DAD shall conform to Single Sign On facility, when that becomes available on DoD networks. See DII COE Security Services SRS.			
3.2.2.2.3.3-2.4.5	DAD shall provide the capability to manage account passwords.			
3.2.2.2.3.3-2.4.5.1	DAD shall provide the capability to create a user account password.			
3.2.2.2.3.3-2.4.5.2	DAD shall provide the capability to modify a user account password.			
3.2.2.2.3.3-2.4.5.3	DAD shall provide the capability to delete a user account password.			
3.2.2.2.3.3-2.4.6	DAD shall provide the capability to generate reports on user accounts.			
3.2.2.2.3.3-2.4.6.1	DAD shall provide the capability to generate reports on user accounts listing, by account privilege, at minimum the user ID, user fullname, user organization, user phone.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.3.3-2.4.7	DAD shall provide the capability for registered users to change passwords.			
3.2.2.2.3.3-2.4.8	DAD shall force users to change passwords after a specified time period.			

3.2.2.2.3.4 DAD License Management Requirements

DAD license management requirements for CM Services software are provided in Table 3.2.2.2.3.4-1.

Table 3.2.2.2.3.4-1. DAD License Management Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.3.4-1	DAD shall provide the capability to identify an asset as needing license verification or not.			
3.2.2.2.3.4-2	DAD shall provide the capability, when license verification is necessary, to initiate a license verification process (e.g., initiate link to external web page explaining the license verification process.).			
3.2.2.2.3.4-3	DAD shall accommodate any DAD-related requirements for DII Enterprise Licensing presented in the License Management SRS when that SRS becomes available.			
3.2.2.2.3.4-4	DAD shall present to the user the licensing restrictions associated with an asset prior to download.			
3.2.2.2.3.4-5	DAD shall link licensing information to assets and prompt the user to accept the license terms and conditions presented prior to download.			
3.2.2.2.3.4-6	DAD shall provide the capability to notify COTS users when their enterprise license is running out.			
3.2.2.2.3.4-7	DAD shall provide the capability for the Asset Manager to qualify potential recipients of enterprise licenses prior to download.			
3.2.2.2.3.4-8	DAD shall provide the capability for automatic download of associated documentation and license information with assets.			

3.2.2.2.3.5 DAD Report Requirements

DAD report requirements for CM Services software are provided in Table 3.2.2.2.3.5-1.

Table 3.2.2.2.3.5-1. DAD Report Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.3.5-1	DAD shall provide reliable, accurate, and timely asset management data and information.			
3.2.2.2.3.5-2	DAD shall provide the capability for any DAD report to be sent to screen, file, or printer.			
3.2.2.2.3.5-2.1	DAD shall provide the capability for any DAD report to be sent to screen.			
3.2.2.2.3.5-2.2	DAD shall provide the capability for any DAD report to be sent to file.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.3.5-2.3	DAD shall provide the capability for any DAD report to be sent to printer.			
3.2.2.2.3.5-3	DAD shall provide the capability for any DAD log to be sent to screen, file, or printer.			
3.2.2.2.3.5-3.1	DAD shall provide the capability for any DAD log to be sent to screen.			
3.2.2.2.3.5-3.2	DAD shall provide the capability for any DAD log to be sent to file.			
3.2.2.2.3.5-3.3	DAD shall provide the capability for any DAD log to be sent to printer.			
3.2.2.2.3.5-4	DAD shall provide the capability to generate standard reports (defined in this SRS), ad hoc reports, and customized reports.			

3.2.2.2.3.6 DAD Reliability, Availability, and Maintainability Requirements

DAD reliability, availability, and maintainability requirements for CM Services software are provided in Table 3.2.2.2.3.6-1.

Table 3.2.2.2.3.6-1. DAD Reliability, Availability, and Maintainability Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.3.6-1	DAD shall provide all required capabilities 24 hours a day, 7 days a week.			
3.2.2.2.3.6-2	DAD shall provide backup and recovery capability.			
3.2.2.2.3.6-2.1	DAD shall provide the capability to schedule backups.			
3.2.2.2.3.6-2.2	DAD shall provide the capability to report the status of a backup.			
3.2.2.2.3.6-2.3	DAD shall log the result of a backup as successful or unsuccessful.			
3.2.2.2.3.6-2.4	DAD shall support partial and complete recoveries.			
3.2.2.2.3.6-2.5	DAD shall log the result of a recovery as successful or unsuccessful.			

3.2.2.2.4 Internal Distribution Requirements

Internal distribution requirements for CM Services software are provided in Table 3.2.2.2.4-1.

Table 3.2.2.2.4-1. Internal Distribution Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.4-1	The system shall provide the capability for internal distribution of segments and documentation received from developers to other activities within DISA, including engineering, integration and test.			

3.2.2.2.5 World Wide Web Information Access and Control Requirements

DISA is currently using their home page for information dissemination and forms and database distribution and collection. In addition, they are currently linked to Services home pages to allow users access to needed data. World Wide Web information access and control requirements for CM Services software are provided in Table 3.2.2.2.5-1.

Table 3.2.2.2.5-1. World Wide Web Information Access and Control Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.5-1	DISA-sponsored web pages that link to CM Services software shall be developed and designed in accordance with the guidelines specified in the *DISA/NCS World Wide Web Handbook*, Version 2.2.			
3.2.2.2.5-2	DISA-sponsored web pages that link to CM Services software shall be developed and designed in accordance with the guidelines specified in DISA Instruction 630-225-7, *Internet, Intranet and World Wide Web*.			
3.2.2.2.5-3	DISA-sponsored web pages that link to CM Services software shall be developed and designed in accordance with the policies specified in the *OSD Policy for Establishing and Maintaining a Publicly Accessible Department of Defense Web Information Service*.			
3.2.2.2.5-4	Web mission-application segments developed for the system shall not include a web-server, but shall use the web server provided by the DII COE.			
3.2.2.2.5-5	All web-based segments shall be DII COE-compliant.			
3.2.2.2.5-6	The system shall provide the capability to publish/post documentation on web pages (both NIPRNET and SIPRNET).			
3.2.2.2.5-7	The system shall be able to identify all documents/files/segments that have been cleared for posting on the classified and unclassified web pages, as well as those that have actually been posted.			
3.2.2.2.5-8	The system shall provide a web-based, dynamic on-line document search capability to allow users to locate documents posted on the web and to download them via the browser.			
3.2.2.2.5-9	The system shall provide the capability to compress files.			
3.2.2.2.5-10	System web segments shall, as a minimum, support HTML 3.2 and frames.			
3.2.2.2.5-11	The system shall provide the capability to create and edit html/text files. The system shall provide an html syntax checker for users to use after an html file has been edited or created. When the syntax checker is activated, an error file shall be created by the system whether errors are found or not. The system shall provide users with the capability to view the contents of the error file in a text editor.			
3.2.2.2.5-12	The system shall provide the capability to identify all html syntax errors and the corresponding file name on any DII COE web site. When the syntax checker is activated, an error file shall be created by the system whether errors are found or not. The system shall provide users with the capability to view the contents of the error file in a text editor.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.5-13	The system shall provide the capability to convert word processing files to PDF format. The system shall provide the capability to combine multiple PDF files into one homogeneous PDF file.			
3.2.2.2.5-14	The system web server shall be able to support HTTP 1.0 and HTTP 1.1 transport protocols.			
3.2.2.2.5-15	The system shall provide a web-based capability to allow authorized users to perform dynamic queries of real time MIS data.			
3.2.2.2.5-16	The system shall provide a web-based capability for users to submit GSPR, Change Request (CR) and PR forms to the MIS using their web browser.			
3.2.2.2.5-17	The system shall provide a web-based capability for authorized users to view the status of GSPRs in the MIS.			
3.2.2.2.5-18	The system shall provide a web-based capability for authorized users to search GSPRs based on search criteria for content and related information such as originator, segment(s) impacted, and scheduled build or version for implementation.			
3.2.2.2.5-19	The system shall provide a web-based capability for authorized users to access segment status information maintained in the MIS database. The system shall provide users with the ability to search for segments by DII COE release.			
3.2.2.2.5-20	The system shall provide a web-based capability for authorized users to view the latest DII COE software release listing. The system shall provide information on DII COE software release media and their respective CM numbers to be used for ordering the media on the web page.			
3.2.2.2.5-21	The system shall provide a web-based capability for authorized users to view the dependencies between DII COE software segments and COTS products. This information assists developers and users in determining what COTS licenses are needed for specific software segments.			
3.2.2.2.5-22	The system shall provide a web-based capability for users to pre-register a DII COE segment prior to delivery to the CFI.			
3.2.2.2.5-23	When registering a DII COE segment using the web, the system shall require the user to enter key points of contact.			
3.2.2.2.5-24	The system shall provide a web-based capability for users to search currently used segment prefixes.			
3.2.2.2.5-25	The system shall provide web-based access to the on-line Delivery Schedule Calendar to authorized users. Users shall be able to view the calendar of scheduled deliveries.			
3.2.2.2.5-26	The system shall provide a web-based capability for authorized users to schedule or modify schedules for software segment deliveries to the CFI.			
3.2.2.2.5-27	The system shall only allow authorized system administrators to make modifications to a particular segment's delivery schedule in the Delivery and Scheduling System when the scheduled delivery time is in less than 48 hours.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.5-28	The system shall provide the capability to determine if there are any incorrect link references made between the GCCS and DII COE web pages and externally maintained web pages. The system shall also provide the capability to determine whether there are any missing links.			
3.2.2.2.5-29	The system shall provide authorized users with the ability to perform web server maintenance.			
3.2.2.2.5-30	The system shall provide web account groups as described in Paragraph 7.2 of the I&RTS.			

The following requirements also apply to Web information access and control capabilities:

3.2.1.2-29	3.2.2.1.10-7	3.2.2.2.14-1
3.2.2.1.3-20	3.2.2.2.2-1	3.2.2.2.14-14
3.2.2.1.6-14	3.2.2.2.3.4-2	3.2.2.2.14-15
3.2.2.1.9-11	3.2.2.2.10-2	3.2.2.3.2-16
3.2.2.1.9-12	3.2.2.2.11-2	3.2.2.3.4-7

3.2.2.2.6 Interface Definition Requirements

Interface definition requirements for CM Services software are provided in Table 3.2.2.2.6-1.

Table 3.2.2.2.6-1. Interface Definition Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.6-1	All internal and external interfaces to DII COE component software shall be identified per Interface Control Document or equivalent standards.			
3.2.2.2.6-2	All internal and external interface requirements to DII COE component software shall be specified per Interface Control Document or equivalent standards.			
3.2.2.2.6-3	All inputs and outputs of the internal interfaces shall be specified per Interface Control Document or equivalent standards.			
3.2.2.2.6-4	All inputs and outputs of the external interfaces shall be specified per Interface Control Document or equivalent standards.			
3.2.2.2.6-5	The system shall provide authorized users with access to established interface agreements between DII COE user organizations.			
3.2.2.2.6-6	The system shall maintain and report the minutes of prior Interface Control Working Groups (ICWGs).			
3.2.2.2.6-7	The system MIS shall track all action items that are established during ICWGs. The MIS shall contain general information about the action item and shall track specific activities and suspenses associated with closing the action item.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.6-8	For each ICWG action item officially established by the Government, the MIS shall establish and keep current a separate record to identify: a. The type of ICWG b. The identification number of the action item c. Short title for the action item d. The date the action item was established e. For each activity identified as required to close out the action item, provide: (1) Identification of the activity (2) Identification of the responsible agency (3) The suspense date for completion of the activity (4) The actual closeout date of the activity.			

3.2.2.2.7 Baseline Information Requirements

Baseline information requirements for CM Services software are provided in Table 3.2.2.2.7-1.

Table 3.2.2.2.7-1. Baseline Information Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.7-1	DII COE software components shall be baselined.			
3.2.2.2.7-2	The types and contents of baselined information shall be identified.			
3.2.2.2.7-3	The system shall provide for storage of and access to documentation that defines the DII COE system and CI baselines for each site.			
3.2.2.2.7-4	Baselined information management shall be automated.			
3.2.2.2.7-5	Using automated means, baseline information shall be captured.			
3.2.2.2.7-6	Using automated means, baseline information shall be maintained.			
3.2.2.2.7-7	Using automated means, baseline information shall be queried.			
3.2.2.2.7-8	Using automated means, baseline information shall be output in the form of reports.			
3.2.2.2.7-9	The system shall provide the capability to maintain and report the status on a CM Baseline Development Checklist of CM actions to be completed prior to each major baseline development event for the system and each CI, as applicable. Checklists shall be maintained to track actions to support development of the following: a. Functional Baseline b. Allocated Baseline c. CI/CSCI Integration d. Major CI/CSCI/System testing events.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.7-10	The CM Baseline Development Checklist shall include the following information for each item listed: a. Event priority b. Event criticality to accomplishment of CM objectives c. Event planned start date d. Event planned end date e. Event actual start date f. Event actual end date d. Reason(s) for schedule changes e. Event completion status (expressed as a percentage, if applicable) f. Event dependencies g. Organization/ Point-of-Contact responsible for coordination and completion of the event h. Event schedule thresholds i. Activities, programs, releases, etc., impacted by changes to event schedule j. Overall impact of changes to event schedule.			

3.2.2.2.8 Controlled Libraries Requirements

Controlled library requirements for CM Services software are provided in Table 3.2.2.2.8-1.

Table 3.2.2.2.8-1. Controlled Libraries Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.8-1	DII COE software and documentation shall be established in the form of controlled libraries.			
3.2.2.2.8-2	The system shall be able to maintain a repository of CI documentation files and enable the user to store and retrieve CI documentation files.			
3.2.2.2.8-3	The DII COE software and documentation to be submitted into the controlled libraries shall be identified.			
3.2.2.2.8-4	The system shall record all of the data known about a particular delivered document/segment as specified in the original delivery letter provided with the document.			
3.2.2.2.8-5	The system shall provide the authorized user with the capability to enter the new items into the appropriate CM libraries with the version number, date, and other information as required. For segment deliveries, the VERSION file gives the current version and the material date of the segment.			
3.2.2.2.8-6	When entering an item into one of the CM Libraries, the system shall provide an automated capability to forward delivery items provided on electronic media to names selected from the CM Point of Contact List.			
3.2.2.2.8-7	When entering an item into one of the CM Libraries (Tape, Document, Segment, License, or Requirement), the system shall provide the capability to determine whether the item is for a new segment or supersedes an existing library asset.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.8-8	The system shall provide automated support for tracking, recording and controlling access to items entered into the Tape, Document, Segment, License, and Requirement Libraries.			
3.2.2.2.8-9	The system shall be able to identify all of the segments associated with a particular document.			
3.2.2.2.8-10	The system shall maintain a record of which segment(s) are provided on which tape for a specific system release. (NOTE: A release may consist of multiple tapes. A segment may be released under several different system releases and a single segment may be placed on multiple tapes for a single system release.)			
3.2.2.2.8-11	The system shall provide an automated capability to create a TAR (Transfer Archive) file of delivered segments and put the file in the segment library.			
3.2.2.2.8-12	The types of access control for the types of controlled libraries maintained shall be identified.			
3.2.2.2.8-13	Access to information on the contents of the segment library shall be password controlled.			
3.2.2.2.8-14	The access control mechanism(s) for each type of controlled library maintained shall be identified.			
3.2.2.2.8-15	The organizations requiring access to the controlled libraries shall be identified.			
3.2.2.2.8-16	The required access control mechanism(s) shall be assigned to each organization depending on the controlled libraries to be accessed.			
3.2.2.2.8-17	The system shall provide the capability to generate and output formatted and ad hoc reports on the contents of any of the CM Libraries.			
3.2.2.2.8-18	The system shall be able to generate and output the Internal request memo for CM library documents that are requested at the CFI.			
3.2.2.2.8-19	The system shall provide an automated capability to generate and print cover pages for delivered documents with the appropriate classification markings.			
3.2.2.2.8-20	The system shall be able to generate and output floppy disk labels.			
3.2.2.2.8-21	The system shall provide an automated capability to generate installable MakeInstall tapes for providing software to Testing and Integration activities and to satisfy customer requests. Support for 4 mm and 8 mm tapes and Compact Disks-Read Only Memory (CD ROMs) shall be provided.			
3.2.2.2.8-22	The system shall provide the capability for authorized users to build scripts (UNIX) to create tapes with multiple segments for release to customers.			
3.2.2.2.8-23	The system shall provide the capability for authorized users to reproduce/duplicate tapes.			
3.2.2.2.8-24	The system shall provide tape utility functions, including, duplicating and rewinding tapes, writing to a tape from a disk, writing to a disk from a tape, specifying directory locations, and moving directories.			
3.2.2.2.8-25	The system shall provide the capability for authorized users to reproduce/duplicate CD ROMs.			

3.2.2.2.9 CI and Tracking Information Access and Control Requirements

CI and tracking information access and control requirements for CM Services software are provided in Table 3.2.2.2.9-1.

Table 3.2.2.2.9-1. CI and Tracking Information Access and Control Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.9-1	The system shall provide users with access to baseline CI data and documentation.			
3.2.2.2.9-2	CI and tracking information that requires access control shall be identified.			
3.2.2.2.9-3	The types of access control for the types of information maintained shall be identified.			
3.2.2.2.9-4	The access control mechanism(s) for each type of information maintained shall be identified			
3.2.2.2.9-5	The organizations requiring access to this information shall be identified.			
3.2.2.2.9-6	The required access control mechanism(s) shall be assigned to each organization depending on the types of information to be accessed.			
3.2.2.2.9-7	The system shall restrict access to system requirements information to only authorized users.			
3.2.2.2.9-8	The system shall provide access controls to qualify who can read or modify system requirements data down to individual attribute values.			
3.2.2.2.9-9	Assigned user permissions shall determine which CI data search and retrieval functions are available to the user.			
3.2.2.2.9-10	CI data search functions, including searches initiated by the report generation capability, shall be password protected.			
3.2.2.2.9-11	The system shall provide the capability for remote access to system requirements information using client/server technology.			
3.2.2.2.9-12	The system shall provide the capability to present requirements information via a web link.			
3.2.2.2.9-13	The system shall include a mechanism to allow query of the document database through the world-wide web. Only those documents identified as releasable shall be visible to web-based queries.			
3.2.2.2.9-14	The system shall automatically generate the documents necessary to fulfill a CI request (tape/document labels, shipping labels, transmittal/receipt forms, interoffice delivery memos).			
3.2.2.2.9-15	The system shall track each CI delivery request through every phase of its life cycle (receipt, fulfillment, shipping).			
3.2.2.2.9-16	The system shall record all of the tasks performed to fulfill a request, who executed the task, and the start/stop times of the task.			
3.2.2.2.9-17	The system shall be able to generate and output the CM Software and Documentation Request Form.			
3.2.2.2.9-18	The system shall be able to generate and output the CM Request LOG form.			
3.2.2.2.9-19	The system shall be able to generate and output the CM Request LOG brief listing form.			
3.2.2.2.9-20	The system shall be able to generate and output the CM Request Report.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.9-21	The system shall be able to generate and output the CM Due Date Report.			
3.2.2.2.9-22	The system shall be able to generate and output the CM Over Due Report.			
3.2.2.2.9-23	The system shall be able to generate and output the CM Your Outstanding Tasks Report.			
3.2.2.2.9-24	The system shall be able to generate and output the CM All Outstanding Tasks Report.			
3.2.2.2.9-25	The system shall be able to generate and output the WEB Not Started Report.			
3.2.2.2.9-26	The system shall be able to generate and output the Form for Email not Start Report.			
3.2.2.2.9-27	The system shall have the capability to configure DII COE software builds that comply with releasability and exportability restrictions for the applicable Foreign Military Sales (FMS) Case.			
3.2.2.2.9-28	In support of software release tape generation, the system shall provide the capability to review tape contents to determine if any releasability and exportability restrictions have been violated. If violations are detected, the system shall have the capability to identify the affected segments and segment versions.			

3.2.2.2.10 License Management Requirements

License management requirements for CM Services software are provided in Table 3.2.2.2.10-1.

Table 3.2.2.2.10-1. License Management Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.10-1	The system shall provide tools to enable single-point COTS license management. License management tools shall be interoperable with other relevant management functions.	4.0	Solaris 2.5.1 & NT4.0+	
3.2.2.2.10-2	The system shall support a web-based capability to publish information on availability of licenses and associated license information. The system shall provide a web interface for authorized users to review available licenses and the associated information and download COTS licenses. The system shall identify who downloaded the licenses and the associated Service/Agency or DoD program.			
3.2.2.2.10-3	The system shall maintain a database of license keys issued to DISA for DISA-purchased products. The system shall record the agency and Point-of-Contact to whom those keys were issued when such software is supplied as part of a DII COE release.			
3.2.2.2.10-4	The system shall provide the capability for license metering for all segmented products requiring license accountability.	4.0	All HP, Solaris, and NT	

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.10-5	The system shall be able to track and report on the number of COTS licenses being downloaded for each COTS product. The system shall identify who downloaded the licenses and the associated Service/Agency or DoD program.			
3.2.2.2.10-6	The system shall be able to identify the number and type of COTS license required to be purchased by the user(s) of any given segment or group of segments.			
3.2.2.2.10-7	The system shall maintain sufficient information on COTS purchases by designated license procurement and distribution Points-of-Contact to support negotiation of favorable licensing arrangements.			
3.2.2.2.10-8	The system shall maintain a database of all COTS/Segment dependencies and Segment/COTS dependencies.			
3.2.2.2.10-9	The system shall identify all segment conflicts with other segments.			

3.2.2.2.11 Request Processing Requirements

Request processing requirements for CM Services software are provided in Table 3.2.2.2.11-1.

Table 3.2.2.2.11-1. Request Processing Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.11-1	The system shall allow for a user-maintainable standard distribution list, through which CI requests can be generated automatically and placed into the fulfillment queue.			
3.2.2.2.11-2	The system shall provide a web-based capability for users to submit on-line requests for DII COE documentation and software from the CM library.			

3.2.2.2.12 Subscriber Lists Requirements

Subscriber lists requirements for CM Services software are provided in Table 3.2.2.2.12-1.

Table 3.2.2.2.12-1. Subscriber Lists Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.12-1	The system shall maintain a record of every segment that has been cleared for Foreign Military Sales (clearance may be limited to only specified countries), as well as recording those segments that have been so released, and the country or countries to which they were released.			

The following requirements also apply to subscriber lists:

3.2.2.1.2-24	3.2.2.2.1-15	3.2.2.2.1-22	3.2.2.2.3.2-8
3.2.2.1.5-4	3.2.2.2.1-21	3.2.2.2.11-1	3.2.2.2.3.2-9

3.2.2.2.13 Ad hoc Distribution Lists Requirements

TBD

3.2.2.2.14 Change Control Requirements

Change control requirements for CM Services software are provided in Table 3.2.2.2.14-1.

Table 3.2.2.2.14-1. Change Control Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.14-1	The system shall provide both local (on-site) and web-based access to electronic copies of blank ECP, SCN, SCP, CR, PR and GSPR forms and instructions for completing each of the forms.			
3.2.2.2.14-2	Change Control procedures for DII COE software components shall be identified.			
3.2.2.2.14-3	Change Control procedures shall be established.			
3.2.2.2.14-4	Change Control procedures shall be established to include Engineering Change Proposals (ECPs).			
3.2.2.2.14-5	Change Control procedures shall be established to include Software Change Notices (SCNs).			
3.2.2.2.14-6	Change Control procedures shall be established to include Global System Problem Reports (GSPRs).			
3.2.2.2.14-7	Change control information management for each DII COE software component shall be automated.			
3.2.2.2.14-8	Using automated means, Change Control information on each DII COE software component shall be captured.			
3.2.2.2.14-9	Using automated means, Change Control information on each DII COE software component shall be maintained.			
3.2.2.2.14-10	Using automated means, Change Control information on each DII COE software component shall be queried.			
3.2.2.2.14-11	Using automated means, Change Control information on each DII COE software component shall be output in the form of reports.			
3.2.2.2.14-12	The system shall support changes to an established baseline and shall be able to apply those changes across CM functions.			
3.2.2.2.14-13	The system shall allow GSPR records to be entered into the database in a preliminary form that will not be included in management reports until validated by the QA chief.			
3.2.2.2.14-14	The system shall provide the capability for PRs to be submitted on-line using a web-based interface (dynamically links into the MIS database) by the Customer Hot Line (GCCS Management Center (GMC)/Sites, GTAC, DII COE), CFI testers, developers and integrators, SSC SD testers, and any other activities associated with the software.			
3.2.2.2.14-15	The system shall provide the capability for authorized users to save GSPRs to an html file for posting/publishing on a web page.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.14-16	The system shall provide the capability for authorized users to update and edit PR and GSPR status information, change the organization assigned to the problem, upgrade/downgrade the priority, change the PR to a Change Request (CR), and close or defer the PR or GSPR.			
3.2.2.2.14-17	The system shall provide the capability for authorized users to elevate a PR to a GSPR.			
3.2.2.2.14-18	The system shall support the life cycle of a GSPR so as to track the progress of all resulting configuration changes or corrective actions, if any, until the problem is either fixed or permanently resolved in some other way.			
3.2.2.2.14-19	The system shall support the life cycle of a System Change Request (SCR) so as to track the progress of all configuration changes.			
3.2.2.2.14-20	The system shall provide the capability to track and maintain information on each of the key elements of information provided in ECPs, SCNs, SCPs, NORs, CRs, PRs and GSPRs in record format to support queries and report generation.			
3.2.2.2.14-21	The system shall provide the capability to automate recording of information in ECPs, SCNs, SCPs, NORs, CRs, PRs and GSPRs provided in electronic format into the MIS.			
3.2.2.2.14-22	The system shall provide the capability to track and maintain information on Requests for Deviation. The system shall track the approval/disapproval status for each deviation request.			
3.2.2.2.14-23	The system shall be able to accept input data in electronic form from the Remedy Action Request System (ARS) which is used to track help desk requests, FormFlow which is used to create standardized forms, and world wide web interfaces.			

3.2.2.2.15 Version Control Requirements

Version control requirements for CM Services software are provided in Table 3.2.2.2.15-1.

Table 3.2.2.2.15-1. Version Control Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.15-1	Each baselined DII COE software component shall be assigned Version Control numbers.			
3.2.2.2.15-2	The form and content of Version Control numbers shall be specified.			
3.2.2.2.15-3	Version Control number management shall be automated.			
3.2.2.2.15-4	Using automated means, Version Control numbers shall be captured.			
3.2.2.2.15-5	Using automated means, Version Control numbers shall be maintained.			
3.2.2.2.15-6	Using automated means, Version Control numbers shall be queried.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.15-7	Using automated means, Version Control numbers shall be output in the form of reports.			
3.2.2.2.15-8	The system shall assist in the tracking of segments released with each system version. As part of this requirement, the system shall generate a shell Release Bulletin containing the data available for every segment that is to be included in a release.			
3.2.2.2.15-9	The system shall maintain a record of supercession of segments.			
3.2.2.2.15-10	The system shall be able to identify all documents (including Computer Based Training items) associated with a particular version of a segment.			
3.2.2.2.15-11	The system shall allow for a prioritization of segments based on Joint Staff provided 'Operational Utility' ranking, to assist in making the determination of whether a particular system version is ready for release.			
3.2.2.2.15-12	The system shall provide the ability for dynamic updates to COTS products in DII COE Releases, including patches and new versions.	3.2	Solaris 2.5.1 & WIN NT 3.51	

3.2.2.2.16 Configuration Control Metrics Requirements

The requirements covered by this section address metrics designed to measure the efficiency of established configuration control processes. Configuration control metrics requirements for CM Services software are provided in Table 3.2.2.2.15-1. (See also Appendix B for overview of metrics management approach.)

Table 3.2.2.2.16-1. Configuration Control Metrics Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.16-1	The system shall provide the capability for authorized users to generate formatted and ad hoc reports, Gantt Charts, and graphs depicting summary and statistical information on the types of problems reported in GSPRs, the types of problems fixed, the specific segments in which the reported defects/deficiencies were found, and the number of fixes made to specific segments.			
3.2.2.2.16-2	The system shall provide the capability for authorized users to generate Gantt Charts and graphs depicting summary and statistical information on the number of new GSPRs, GSPR originators, the number of approved and disapproved GSPRs, the number of unfinanced and financed GSPRs, the number of GSPRs satisfied and closed in DII COE Build Plans and Releases, the amount of time required for GSPR processing tasks, GSPR cost to implement, GSPR priority, and the number of GSPRs linked to test procedures.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.16-3	The system shall provide the capability to track and report on the amount of time required for GSPR processing tasks according to GSPR priority and level of effort, to include the following: a. From receipt of PR to PR's approval as a GSPR b. From GSPR preliminary validation to Preliminary Configuration Review Board (PCRB)/Local Configuration Control Board (LCCB) Review c. From GSPR Formal validation (by PCRB/LCCB) to GSPR disapproval. d. From GSPR Formal validation (by PCRB/LCCB) to GSPR approval, assignment to a build and responsibility assignment (per developer) e. From GSPR approval/assignment to a build to GSPR complete fix and implementation in software (per developer).			
3.2.2.2.16-4	The system shall provide the capability to compare the number of ECPs targeted for each DII COE release with the actual number of ECPs incorporated and verified by testing.			
3.2.2.2.16-5	The system shall provide the capability to track and report on the amount of time required for ECP processing tasks according to ECP priority and level of effort. Intervals to be measured and tracked include: a. ECP cycle time from determination of need until ECP is requested or initiated b. ECP request/initiation to submittal c. ECP submittal to review by Government CCB d. ECP review by Government CCB to CCB approval e. CCB approval of ECP to contractual direction/modification f. Contractual direction/modification to submittal of modified software g. Contractual direction/modification to submittal of modified technical documentation, as appropriate			
3.2.2.2.16-6	The system shall provide the capability to track and report on the rate at which ECPs are approved according to ECP priority and level of effort. The system shall be able to track and report on the rate of ECP first pass approvals in any time period by counting the number of ECPs approved upon first submittal to a CCB and divide by the total number of ECPs submitted. (Do not count the number of ECPs that are revised and resubmitted.)			
3.2.2.2.16-7	The system shall provide the capability for authorized users to generate formatted and ad hoc reports, Gantt Charts, and graphs depicting summary and statistical information on requests for deviation, including the number of deviation requests in any given time period, the number of times that a deviation recurs (i.e., requested for a second or third iteration), and the number of deviation requests against specific segments/CSCIs, documentation requirements, and incorporation of approved changes.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.16-8	The system shall provide the capability to track and report on the number of times DII COE software segments and releases were distributed electronically versus on electronic media such as tapes. The system shall provide the capability for these reports to be in the form of graphs, charts, and formatted and ad hoc reports.			
3.2.2.2.16-9	The system shall provide the capability to track and report on requests for DII COE assets by unauthorized users. The system shall track the number of unauthorized user requests, who initiated the request, and the software segments that were requested.			
3.2.2.2.16-10	The system shall provide the capability for authorized users to generate tabular formatted and ad hoc reports depicting event information tracked in the Segment Processing Schedule.			
3.2.2.2.16-11	The system shall provide the capability for authorized users to generate Gantt Charts and graphs depicting the differences between the original plan and subsequent changes in event data tracked in the Segment Processing Schedule. This includes the ability to generate charts, graphs and reports depicting changes and delays in scheduled segment processing events from event information tracked in the Segment Processing Schedule.			
3.2.2.2.16-12	The system shall provide the capability for authorized users to generate Gantt Charts, graphs and formatted and ad hoc reports depicting the differences between the original plan and subsequent changes in event data tracked in the CM Baseline Development Checklist.			

3.2.2.3 Configuration Status Accounting Requirements

3.2.2.3.1 Data Tracking and Recording Requirements

Data tracking and recording requirements for CM Services software are provided in Table 3.2.2.3.1-1.

Table 3.2.2.3.1-1. Data Tracking and Recording Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.1-1	The types and content of configuration status data shall be identified.			
3.2.2.3.1-2	Where the configuration status data are being tracked and recorded shall be identified.			
3.2.2.3.1-3	The frequency the configuration status data are collected, recorded, and queried shall be identified.			
3.2.2.3.1-4	How the configuration status data are being tracked, recorded, and queried shall be identified.			
3.2.2.3.1-5	The organization that tracks, records, and queries the configuration status data shall be identified.			
3.2.2.3.1-6	The volume of configuration status data to be tracked, recorded, and queried shall be identified.			
3.2.2.3.1-7	The system shall identify all proprietary and restricted data and the CIs to which it applies.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.1-8	For each specification prepared and maintained for DII COE to describe and control the performance and/or design of DII COE and its component CIs (hardware and software), a record shall be established in the MIS and kept current. The record shall show: a. The specification ID number b. The specification title c. The Commercial And Government Entity (CAGE) code for the design activity d. The CI nomenclature e. The current revision letter and date of issue f. The most current approved SCN number g. The date of the SCN approval h. The related ECP number i. The contract number and CDRL sequence number.			
3.2.2.3.1-9	The MIS shall maintain a historical file of the information in requirement 3.2.2.3.1-8 for each revision of each CI specification from the date of initial release of the basic specification through the current revision and SCN.			
3.2.2.3.1-10	For each drawing (or equivalent electronic record) that is prepared and maintained to describe the parts used to support the system and its component CIs, a record shall be established in the MIS and kept current. The record shall show: a. The drawing number b. The CAGE Code for the design activity c. The drawing title d. The current revision level e. The part number(s) of the part(s) changed as a result of that drawing change and the effectivity of the part(s) in terms of CI serial numbers f. The ECP number effecting the change, where applicable, and the identifier of the contractor's change document effecting the detailed change to the software and associated documentation g. The effective release date h. The contract number and CDRL sequence number.			
3.2.2.3.1-11	The MIS shall maintain a historical file of the information in requirement 3.2.2.3.1-10 for each drawing revision from the date of release through the current revision.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.1-12	For each software CI purchased/created and maintained for the operation and maintenance of DII COE and its component CIs, a record shall be established in the MIS and kept current. The record shall show: a. The software identification number b. The related CSCI specification number and title c. The CSCI's Government acquisition activity/sponsor d. The CAGE Code for the design activity e. The software title f. The current version and interim version level g. The source code and object code components/units that comprise the CI h. The ECP number effecting the change, where applicable, and the identifier of the contractor's change document effecting the detailed change to the software and associated documentation i. The effective release date of the current version/ interim version j. The number, title, version and date for the current operations/programmers/maintenance manuals and version description document k. The number, title, version and date for the current test procedures l. If the software is resident on a "read only" device (e.g., Programmable Read Only Memory (PROM)), the current part number for the software/medium combination m. The contract number and CDRL sequence number.			
3.2.2.3.1-13	The MIS shall maintain a historical file of the information in requirement 3.2.2.3.1-12 for each version and interim version of the software from the date of initial release of the software through the current revision.			
3.2.2.3.1-14	For each hardware CI, a record shall be generated in the MIS and kept current identifying the CI by name and identifier. The record shall also identify the number, name and CAGE code for all hardware parts/assemblies and sub-assemblies that comprise the CI. It shall be presented in a hierarchical manner so that the "level of assembly" relationships of the various pieces of the CI can be understood by looking at the arrangement of the record. As a minimum, the record shall list all parts/logical units that have been selected by the government for logistics support and all components of those parts that have been selected as spares, including those of superseded but still used configurations.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.1-15	For each active contract affecting the program, a record shall be established in the MIS and kept current. Contracts to be monitored include those that have been issued by the primary Government activity for the DII COE (e.g., development, long-lead, production, and spares) or by other Government activities (e.g., separate spares buys, Government Furnished Equipment (GFE), and modifications) and for which all work and/or deliveries have not yet been completed. Each record shall include: a. The contract number b. The CAGE Code of the contractor c. The CI identifiers, nomenclature(s), or part number(s) of the top level assembly(s) being delivered under the contract d. The number of units to be delivered under the contract.			
3.2.2.3.1-16	For each change idea initiated by either the contractor, the government, or DII COE users, a separate record shall be established in the MIS and kept current. Each record shall identify: a. The type of change involved (e.g., ECP, deviation/ waiver) b. The change identification number (e.g., ECP number) c. The CAGE Code of the originator d. The change title e. The Government acquisition activity/sponsor for the change, if applicable f. The configuration baseline(s) affected g. The title and number of the affected specification(s) h. The related SCN/NOR number i. The priority j. The date on which the change was transmitted to the Government k. The "need date" for a decision on the change l. The final CCB decision m. The date on which the official decision notification was provided to the contractor.			
3.2.2.3.1-17	The MIS shall maintain a historical file of the information in requirement 3.2.2.3.1-16 for each change document submitted to the Government throughout the life of the contract.			
3.2.2.3.1-18	For each change tracked per requirement 3.2.2.3.1-16, the system shall identify and suspense the discrete activities involved in the review of the change by the Government. The system shall automatically assign suspense dates by which those activities must be completed, based on the need date and the priority of the change. The Government's change manager shall have the capability to change suspense dates (except the need date) and to input completion dates reflecting the status of the processing of the change.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.1-19	For each change tracked per requirement 3.2.2.3.1-16, the system shall be capable of tracking and recording the following event dates: a. Change receipt date b. Date change was distributed for coordination/ comments c. Date that coordination/comments are due d. Technical meeting date e. Date corrections to change proposal due from the contractor f. CCB date g. Date that directive is sent to contracting h. Design activity's need date i. Date that contract modification was issued.			
3.2.2.3.1-20	For each change tracked per requirement 3.2.2.3.1-16, when a specific beginning and end date are specified by the originator, the system shall have the capability to provide information (as a calendar listing sorted by day) about all scheduled, but not yet completed, events during that time span. Likewise, when an "as of" date is specified by the originator, the system shall have the capability to identify all scheduled, but not yet completed, events that should have been accomplished by that date and to sort them by magnitude of their delinquency.			
3.2.2.3.1-21	The system MIS shall document the initial approved configuration of each CI and identify the impact of each approved, contractually authorized Class I and Class II change to the approved configuration.			
3.2.2.3.1-22	For each CI, a historical record documenting all of the changes that have been approved against that CI shall be established in the MIS and kept current. The record shall reflect: a. The change identification number b. The CAGE Code of the originator (plus for Class I ECP changes the identification of the Government procuring activity) c. The title of the change d. The date of the approval of the change e. The contract modification number, if appropriate f. The complete unit serial number effectivity (or the month and year of implementation for Class II changes) g. The serial numbers of already delivered units to be modified as a result of the change h. The new part numbers and/or drawing revision levels and/or new software component/unit versions (and related affected manuals) resulting from each approved change i. The contract number and CDRL sequence number.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.1-23	The MIS shall track the accomplishment of all tasks required as a result of all approved change proposals. The system shall include key elements of information about each change, including the functional activities responsible for the accomplishment of the tasks. The system shall have the capability to establish and track scheduled and actual dates for the accomplishment of the various tasks involved in the implementation of each approved change.			
3.2.2.3.1-24	For each change approved against DII COE or one of its component CIs, the record established in requirement 3.2.2.3.1-22 shall include specific suspense dates and actual dates for the completion of all activities related to each of the major areas of impact of the change. The record shall also identify the specific point of contact responsible for each activity, including their phone number and e-mail address. As appropriate to the change involved, these activities include, but are not limited to, the following: a. Status of redesign and testing b. Specification change/revision activity c. Drawing revision activity d. Software revision activity e. Technical manual preparation/revision f. Spares purchase and distribution g. Support equipment design, purchase, or modification h. Retrofit/modification kit development i. The contact number and CDRL sequence number.			
3.2.2.3.1-25	For each change approved against DII COE or one of its component CIs, each implementation area tracked in the record from requirement 3.2.2.3.1-22 shall be expanded as identified in the contract. It shall specify the discrete activities leading to the completion of the work in that specific implementation area, and it shall include the suspense dates and actual dates for the completion of each of those discrete activities. Activities for which this information shall be tracked in the MIS include: a. Specification change/revision activities b. Drawing revision activities c. Software revision activities d. Technical manual and other related document preparation/revision activities e. Spares purchase and distribution activities f. Support equipment design, purchase or modification activities g. Retrofit/modification kit development activities.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.1-26	If an approved change has affected a specification, the record established for requirement 3.2.2.3.1-22 shall track the activities required to distribute the official SCN to holders of the specification in the field. If the approved change results in a revision to the specification, the record shall track the similar activities required to distribute the revised specification. Discrete events and associated dates that shall be tracked include: a. Approval copy prepared (update of originals) b. Copy submitted to Government c. Copy approved by the Government d. Approved copy received by the contractor e. SCN and pages distributed to all addressees.			
3.2.2.3.1-27	If an approved change has affected a drawing, the record established for requirement 3.2.2.3.1-22 shall track revision, review and official release of the drawing incorporating the change. Discrete events and associated dates that shall be tracked include: a. Receipt of approved change document b. Drafting of official drawing changes c. Review and approval by appropriate TWG d. Review and approval by Architecture Oversight Group-Executive Session (AOG-ES) e. Review and approval by CRCB f. Release of new document g. Revised drawings distributed to all addressees.			
3.2.2.3.1-28	If an approved change has affected a software unit, the record established for requirement 3.2.2.3.1-22 shall track the revision, review and official release of the DII COE software release incorporating the change. Such tracking shall be used for software used in the operation of DII COE, in the maintenance of DII COE, and/or in trainers and simulators for DII COE. Discrete events and associated dates that shall be tracked include: a. Receipt of approved change document b. Coding, checkout, and testing of the software changes c. Revision of affected manuals d. Review and approval by appropriate TWG e. Review and approval by the appropriate Engineering Office f. Approval/concurrence by Government representative g. Release of new software version h. Update of software development library materials i. Reproduction on appropriate medium (e.g., floppy disk, cassette, tape, electronic link) j. Revised code and manuals distributed to all addressees.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.1-29	If an approved change requires revision of the information in various manuals written for the operation or maintenance of the CI, the new instructions must be available when deliveries of the new design to the field are started or when modification kits are delivered to the field. The record established for requirement 3.2.2.3.1-22 shall track the events (and associated dates) leading to the publication and distribution of the new instructions and shall include: a. Technical writing of the revision b. Verification of the instructions c. Revalidation of the technical manual d. Transmit original to control activity e. Reproduction of the required copies f. Distribution of the copies to all addressees.			
3.2.2.3.1-30	If an approved change requires new spare parts to be stocked, the record established for requirement 3.2.2.3.1-22 shall track the events (and associated dates) required to provide them to the support organizations and shall include: a. Old and new part numbers b. Quantity of new spares required c. Design Change Notice (DCN) number d. DCN issued to logistics activity e. Purchase/work order issued f. Parts received from manufacturing activity g. Parts shipped to support activity h. Parts received by support activity.			
3.2.2.3.1-31	If an approved change requires the development or purchase of new support equipment, the record established for requirement 3.2.2.3.1-22 shall track the events (and associated dates) required to provide the support equipment to the supporting activities in time to support the new configuration. Discrete events and associated dates that shall be tracked include: a. Quantity required b. Purchase/work order issued c. Issuance of requirements documentation d. Redesign, or new design, work completed e. Prototype constructed f. Testing completed g. Final CCB approval h. Update Engineering Release Records i. Production started j. Deliveries to Government.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.1-32	If an approved change requires that the new configuration approved for the production line be retroactively incorporated (retrofitted) into the units and/or support equipment already accepted by the Government, the record established for requirement 3.2.2.3.1-22 shall track the events (and associated dates) required to develop the kit of parts and the associated instructions. Discrete events and associated dates that shall be tracked include: a. Quantities of kits for delivered units b. Quantities of kits for spare units c. Quantities of kits for training sets d. Purchase/work order issued e. Parts delivered by manufacturing activity f. Installation instructions drafted g. Installation instructions verified h. Validation (proofing) of kit and instructions i. Delivery of kits to support activity.			
3.2.2.3.1-33	The MIS shall document the exact configuration of each unit delivered to the site, as well as certain specifically identified critical components of each unit, and track changes to the configuration of each unit and component. Certain critical components of each unit shall be tracked by both part number and serial number. The system shall be capable of identifying the exact configuration of each unit of the CI and of identifying the total number of units having a specific configuration. Where continuing operational use of more than one configuration of a CI is approved, the system shall identify all currently approved configurations and the quantities of each configuration in operational use.			
3.2.2.3.1-34	As each unit of a CI is manufactured and delivered to the Government, an “as-built” record shall be established in the MIS for the Government detailing the exact configuration.			
3.2.2.3.1-35	For hardware configuration items (HWCIs), the as-built data shall correlate to the as-designed engineering data and manufacturing/quality records. The as-built data record (Requirement 3.2.2.3.1-34) shall include: a. The verified detailed composition of the item in terms of subordinate HWCIs and subordinate parts, associated serial/lot numbers, and, where applicable, engineering changes incorporated b. The variance from as-designed configuration c. The design activity CAGE Code for the HWCI(s) and the part(s) d. For part(s) with proprietary or restricted rights, or for which licensing agreements apply, a record of the documents that specify the limitations, and their associated design activity CAGE Codes, shall be provided.			
3.2.2.3.1-36	For CSCIs, the record (Requirement 3.2.2.3.1-34) shall provide the Version Description Document (VDD) number and where the CSCI is installed.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.1-37	For each unit delivered to the field/site, the record of as-built history (Requirement 3.2.2.3.1-34) shall be updated with information reflecting maintenance actions performed on the unit. The record shall reflect the part number and, where applicable, the serial number of any part replaced in the unit by maintenance action.			
3.2.2.3.1-38	For each unit delivered to the field/site, the record of as-built history (Requirement 3.2.2.3.1-34) shall be updated with information reflecting the retroactive installation (retrofits or modifications) of new design parts in the unit. The record shall reflect: a. The most current part number and name b. The serial number of the part currently installed in that unit			
3.2.2.3.1-39	The system MIS shall track all action items that are established as part of the functional and physical configuration audits for all DII COE configuration items. The MIS shall contain general information about the action item and the article that it affects and shall track specific activities and suspenses associated with closing the action item. The system shall be capable of providing cross-correlation of all action items to be able to present the current status of all action items relating to a specific audit for a specific configuration item.			
3.2.2.3.1-40	For each action item officially established by the contractor and the Government at each configuration audit for DII COE, the MIS shall establish and keep current a separate record to identify: a. The identification number of the CI affected b. The type of audit c. The identification number of the action item d. Short title for the action item e. The date the action item was established f. Contractual and/or specification requirement affected g. For each activity identified as required to close out the action item, provide: (1) Identification of the activity (2) Identification of the responsible agency (3) The suspense date for completion of the activity (4) The actual closeout date of the activity.			
3.2.2.3.1-41	The MIS shall maintain a historical file of the information specified in Requirement 3.2.2.3.1-40, organized by configuration item and by audit type, throughout the life of the contract.			
3.2.2.3.1-42	For each DII COE software release, the MIS shall track MOUs/MOAs associated with FMS cases and with other DoD organizations. For each MOU/MOA, the MIS shall track: a. Organizations involved b. Organizational Points-of-Contact c. MOU/MOA date d. Restrictions for DII COE software use.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.1-43	The MIS shall track the current releasability status for each software CI purchased/created and maintained for the operation and maintenance of DII COE and its component CIs. For each software CI, the MIS shall track the following information: a. Software CI Owner b. Software CI Executive Agent c. Software CI Point-of-Contact d. Point-of-Contact Phone Number e. Releasability Status f. Dates that current releasability status is effective g. Countries to which software CI is releasable h. Countries to which software CI has been sent i. Applicable FMS Case Identification Numbers.			
3.2.2.3.1-44	For each software CI designated as non-releasable, the MIS shall provide the capability to track the reason the software CI is non-releasable and options, if any, for possibly making the software CI releasable.			
3.2.2.3.1-45	The system shall provide the capability to create and maintain MIS data dictionaries, entity relationship diagrams, module structure diagrams, and other documents necessary to plan, implement, and maintain the MIS.			

3.2.2.3.2 CI and System Status Monitoring Requirements

CI and system status monitoring requirements for CM Services software are provided in Table 3.2.2.3.2-1.

Table 3.2.2.3.2-1. CI and System Status Monitoring Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.2-1	The system shall be able to effectively track the status of every software segment in the system through every point in its life cycle.			
3.2.2.3.2-2	DII COE CM activities shall include status accounting of identified CIs such that operational status of its systems can be determined.			
3.2.2.3.2-3	DII COE Application Developers shall include in their documentation information about critical thresholds, dependencies, and processes associated with their application so that they may be monitored once operational.			
3.2.2.3.2-4	The system shall be able to monitor CIs during DII COE system operation and report on CI performance in comparison with documented critical thresholds, dependencies and processes.			
3.2.2.3.2-5	The system shall maintain and report on information on CI critical thresholds, dependencies, and processes.			
3.2.2.3.2-6	The system shall provide a repository of known dependencies (e.g., thresholds, waivers, monitors, etc.) that can be updated when necessary.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.2-7	The system shall provide status information regarding the health and operations of interfaces between managed regions.			
3.2.2.3.2-8	The systems shall maintain and report on the following DII COE system information: a. Product configuration status b. Configuration Documentation c. Current baselines d. Historic baselines e. Change Requests f. Change Proposals g. Change Notices h. Deviations/Requests for Deviation i. Warranty data/history j. Configuration verification and audit status/action item close-out.			
3.2.2.3.2-9	The system shall provide CM TWG members with the capability to query the status of any and all segments associated with any specified DII COE software release.			
3.2.2.3.2-10	The system shall allow for recording results of multiple iterations of three levels of testing (Integration/Compliance/Functional) performed against any Segment/OS/Kernel combination. The system shall provide an on-line system for recording the results of integration testing.			
3.2.2.3.2-11	The system shall allow for a user-maintainable segment grouping/dependency system. Whenever a segment fails any level of testing, dependent/grouped segments will be flagged to indicate the potential for problems.			
3.2.2.3.2-12	The system shall be able to test adherence to waiver conditions.			
3.2.2.3.2-13	The system shall allow for recording of test resources expended against each segment/OS/kernel combination. Multiple testers may be dedicated to any single segment in any phase of testing.			
3.2.2.3.2-14	The system shall be able to compare configuration information extracted during DII COE system backups against the established release baseline and generate a formatted display of the results.			
3.2.2.3.2-15	The results from comparing configuration information extracted during DII COE system backups against the established release baseline shall indicate whether system CIs are the current approved version, an incorrect version, or an unknown segment.			
3.2.2.3.2-16	The results from comparing configuration information extracted during DII COE system backups against the established release baseline shall be able to be displayed on the designated Web server.			

3.2.2.3.3 Build List Status (Per Platform) Requirements

Build list status requirements for CM Services software are provided in Table 3.2.2.3.3-1.

Table 3.2.2.3.3-1. Build List Status (Per Platform) Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.3-1	A Build List of DII COE software components for each DII COE-compliant operating system platform shall be developed.			
3.2.2.3.3-2	The Build Lists shall be coordinated between the DISA Engineering office, DISA Configuration Management office, and the appropriate DII COE Management Boards, Groups, and Subpanels.			
3.2.2.3.3-3	The Build Lists shall be maintained using automated means.			
3.2.2.3.3-4	The Build Lists shall be accessible.			
3.2.2.3.3-5	The Build Lists shall be capable of being populated.			
3.2.2.3.3-6	The Build Lists shall be capable of being queried.			
3.2.2.3.3-7	The Build Lists shall be capable of being output in report format.			
3.2.2.3.3-8	The types of access to the Build Lists shall be identified.			
3.2.2.3.3-9	The types of access control mechanisms for the Build Lists shall be identified.			
3.2.2.3.3-10	The organizations requiring access to the Build Lists shall be identified.			
3.2.2.3.3-11	The access control mechanisms for each organization requiring access to the Build Lists shall be identified.			

3.2.2.3.4 Configuration Change Status Requirements

Configuration change status requirements for CM Services software are provided in Table 3.2.2.3.4-1.

Table 3.2.2.3.4-1. Configuration Change Status Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.4-1	The system shall provide the capabilities to store, uniquely identify, and maintain the status on all DII COE software change requests, problem reports.			
3.2.2.3.4-2	The system shall provide the capability to query and generate customized reports on Change Requests and Problem Reports being tracked based on search criteria for Change Request/Problem Report content and related information such as originator, segment(s) impacted, and scheduled build or version for implementation.			
3.2.2.3.4-3	The system shall provide the capability to apply filters and to conduct searches to identify Change Requests and Problem Reports that meet specified criteria and conditions and output the results in a user-specified output format.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.4-4	Change Request and Problem Report search functions, including searches initiated by the report generation capability, shall be password protected.			
3.2.2.3.4-5	The system shall be able to store, query, and report all relevant problem report information as defined by the DISA Form 291, Global System Problem Report (GSPR).			
3.2.2.3.4-6	The system shall be able to store, query, and report all actions taken to resolve a problem. These actions will include but not be limited to: a historical record of problem statuses; a historical record of each person or group to which a GSPR is assigned for action; and providing a complete textual description of all actions taken to resolve the problem.			
3.2.2.3.4-7	Entries of actions taken to resolve a problem may be generated from information provided by the software developer or vendor, an appropriate review board, the action assignee, or representatives from Integration or Testing. Entries must be brief, concise, yet comprehensive. As each discrete entry is made, it will be captured and stored in such a manner as to allow only the latest entry for each GSPR to be published on an HTML web page.			
3.2.2.3.4-8	The system shall be able to generate and output Miscellaneous Database Reports: Must provide printed reports containing all data elements relevant to a GSPR. These reports must be capable of generation by: a. specific GSPR ID (CM-assigned control number) b. a user-entered list of GSPR IDs c. predefined problem area codes.			
3.2.2.3.4-9	In addition, the above specified GSPR tracking reports (3.2.2.3.4-8) must each allow selectable parameters to include but not limited to: 1. Site ID 2. System Release 3. Priority range 4. Disposition code list 5. Problem Report, Change Report, or both.			
3.2.2.3.4-10	The system shall be able to support the management of GSPRs against itself.			
3.2.2.3.4-11	The system shall track GSPR priorities and targeted releases for the fixes including release for fix to appear, per system engineers			
3.2.2.3.4-12	The system shall be able to identify which changes have already been incorporated into a particular software build and version of a DII COE system CI, and identify those changes that are scheduled for implementation into later builds/versions of the CI.			
3.2.2.3.4-13	The system shall maintain and report on the effectivity and installation status of configuration changes to all DII COE system CIs.			
3.2.2.3.4-14	The system shall record and report configuration changes resulting from retrofit and by replacements through maintenance action.			
3.2.2.3.4-15	The system shall store a repository of approved waivers that can be updated when necessary.			

3.2.2.3.5 Change Accountability Requirements

Change accountability requirements for CM Services software are provided in Table 3.2.2.3.5-1.

Table 3.2.2.3.5-1. Change Accountability Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.5-1	The system shall be able to uniquely identify every problem reported against DII COE, identifying where defects/problems were found (e.g. delivery, integration, testing, release packaging, site installations, field reports) and summarize.			
3.2.2.3.5-2	The system shall be able to categorize reports as either Problem Reports or Engineering Change Requests and support separate management tracks depending on the report type.			
3.2.2.3.5-3	The system shall enable the user to trace all changes (Change Requests, ECPs and Problem Reports) that have been incorporated into each CI as well as the specific modifications made to the CI as a result of the changes.			
3.2.2.3.5-4	The system shall provide traceability of all changes from the original released configuration documentation of each DII COE system CI.			
3.2.2.3.5-5	DII COE software change requests and problem reports shall be traceable to the DII COE segment(s) and baseline documentation affected by the request/report.			
3.2.2.3.5-6	The system shall allow for a hierarchy of system components against which GSPRs can be generated and queried.			
3.2.2.3.5-7	The system shall be able to cross reference a GSPR with tracking numbers assigned to it by other agencies including GMC, GTAC, and the reporting site.			
3.2.2.3.5-8	The system shall have enough tracking states that the life cycle status of the GSPR can be identified in meaningful terms. The system shall allow for the addition/deletion of state codes as the management process evolves.			
3.2.2.3.5-9	The system shall include a mechanism for associating a GSPR with a pre-defined list of CSCIs, Software Applications, Segment Names, and release build list (per system engineers). The system shall also include appropriate mechanisms for maintaining these pre-defined lists.			
3.2.2.3.5-10	The system shall be linked to the GSPR system in such a way that the GSPRs against a segment can be identified.			
3.2.2.3.5-11	The system shall provide links to related GSPRs/problems/defects.			
3.2.2.3.5-12	The system shall include a GSPR tracking mechanism for identification, classification, and management of multiple GSPRs that describe a single problem.			
3.2.2.3.5-13	The system shall include a GSPR tracking mechanism for allowing a common analysis text entry to be electronically entered to multiple problem reports simultaneously.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.5-14	The system shall include a GSPR tracking mechanism for the maintenance of standard valid data elements to include but not limited to: a. site ID values b. system release identifier values c. operating system identifier values d. priority values e. software life cycle phase values f. supplemental material type codes g. status codes h. disposition codes i. assignment group values j. assignment individual k. activity where GSPR was originated (defect found): delivery, integration, segment test, multi-node test, other test, packaging for distribution, site installations, field reports, hot-line, etc.			
3.2.2.3.5-15	The system shall provide the ability to record the transfer of a new GSPR to its responsible agent.			
3.2.2.3.5-16	The system shall provide the capability to generate a GSPR Report showing: Projected fixes for each open GSPR organized by software area to include the current disposition state, the priority, the control number, the System release ID, the site ID, and a set of columns depicted expected future releases. An 'X' will appear under the appropriate future release column to indicate in which future release the problem is expected to be resolved. This report must allow selectable parameters to include but not limited to: a. Disposition code list b. Software area code c. System Release d. Priority range.			
3.2.2.3.5-17	The system shall provide the capability to generate a GSPR Report containing the control number, the control number of any known duplicate GSPRs, the site ID, the priority as submitted and as specified by board review, the current status code, the projected release ID in which this problem is expected to be resolved and the projected release date, the problem title, and the last comment/analysis entry for this GSPR. This report must allow selectable parameters to include but not limited to: a. Disposition code list b. Software area code c. System Release d. Problem Report, Change Report, or both e. Priority range.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.5-18	The system shall provide the capability to generate a GSPR Report containing the control number, the control number of any known duplicate GSPRs, the site ID, the priority as submitted and as specified by board review, the current status code, the projected release ID in which this problem is expected to be resolved, the problem title, and the group and person to which action for this GSPR is currently assigned. This report must allow selectable parameters to include but not limited to: a. Disposition code list b. Software area code c. Site ID d. System Release e. Problem Report, Change Report, or both f. Priority range.			
3.2.2.3.5-19	The system shall provide means to track Problem Reports (PRs) and to associate those PRs to any defined monitor, dependency, or waiver.			

3.2.2.3.6 Inventory of Libraries Requirements

Inventory of libraries requirements for CM Services software are provided in Table 3.2.2.3.6-1.

Table 3.2.2.3.6-1. Inventory of Libraries Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.6-1	Each Build List shall have an associated set of software and documentation libraries.			
3.2.2.3.6-2	Each Build List software and documentation library shall be inventoried.			
3.2.2.3.6-3	The types of access to the Build List software and documentation libraries shall be identified.			
3.2.2.3.6-4	The types of access control mechanisms for the Build List software and documentation libraries shall be identified.			
3.2.2.3.6-5	The organizations requiring access to the Build List software and documentation libraries shall be identified.			
3.2.2.3.6-6	The access control mechanisms for each organization requiring access to the Build List software and documentation library shall be identified.			
3.2.2.3.6-7	The system shall be able to identify the Current Document Change Authority (CDCA) for all design documents and specifications being maintained in the document library.			

The following requirements also apply to inventory of libraries:

3.2.2.2.8-17 3.2.2.4.2-1

3.2.2.3.7 Status Accounting Information Access and Control Requirements

Status accounting information access and control requirements for C M Services software are provided in Table 3.2.2.3.7-1.

Table 3.2.2.3.7-1. Status Accounting Information Access and Control Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.7-1	The system shall provide the capability to designate "Controlled Communities of Interest" and the associated privileges and access permissions.			
3.2.2.3.7-2	The system shall provide users with access to baseline CI status accounting data and documentation.			
3.2.2.3.7-3	The system shall restrict access to system status accounting information to only authorized users.			
3.2.2.3.7-4	The system shall provide access controls to qualify who can read or modify system status accounting data down to individual attribute values.			
3.2.2.3.7-5	CI status accounting data search functions, including searches initiated by the report generation capability, shall be password protected.			
3.2.2.3.7-6	Assigned user permissions shall determine which CI status accounting data search and retrieval functions are available to the user.			
3.2.2.3.7-7	The system shall provide the capability for remote access to system status accounting information using client/server technology.			
3.2.2.3.7-8	The system shall provide the capability to present status accounting information via a web link.			

3.2.2.3.8 Configuration Status Accounting Metrics Requirements

The requirements covered by this section address metrics designed to measure the efficiency and accuracy of established configuration status accounting processes. Configuration status accounting metrics requirements for CM Services software are provided in Table 3.2.2.3.8-1. (See also Appendix B for overview of metrics management approach.)

Table 3.2.2.3.8-1. Configuration Status Accounting Metrics Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.8-1	DII COE Configuration Management shall include the identification of potential problem areas within the DII COE status accounting process.			
3.2.2.3.8-2	Metrics shall be identified with which to classify, verify, and validate problem areas.			
3.2.2.3.8-3	Potential solutions to manage problem areas shall be identified to capture, analyze, and report on the problem areas.			
3.2.2.3.8-4	As appropriate, resources shall be allocated to implement problem area solutions.			
3.2.2.3.8-5	Metrics to evaluate problem area solutions shall be developed to measure the effectiveness of the solutions.			
3.2.2.3.8-6	As appropriate, reallocation of resources shall occur to help support problem area solutions.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.8-7	The system shall be able to generate and output metrics for PRs, including the types of problems reported in PRs, the number of PRs elevated to GSPRs, the number of PRs not elevated to GSPRs, the types of problems fixed, the specific segments in which the reported defects/deficiencies were found, and the number of fixes made to specific segments.			
3.2.2.3.8-8	The system shall be able to track DII COE system thresholds and generate reports, graphs and charts comparing specified DII COE system thresholds with system performance parameters observed during various software testing activities, including integration test, compliance test, and interoperability testing.			
3.2.2.3.8-9	The system shall provide a means of determining any dependency violations (e.g., thresholds, waivers, monitors, etc.).			
3.2.2.3.8-10	The system shall have the ability to report metrics on dependencies including violations of CI performance thresholds and established system configuration baselines.			

3.2.2.4 Configuration Audit Requirements.

Although formal Physical Configuration Audits (PCAs) and Functional Configur ation Audits (FCAs) may not be performed in this system, the MIS database products will allow informal 'audits' or looks at what versions and/or types of CI's and documentation are available when making planning decisions. In addition, DISA will perform internal audits of changes in the system. CM Services software will control changes to the selected CIs, assuring the correct changes are made.

3.2.2.4.1 Site and Configuration Audit Support Requirements

Site and configuration audit support requirements for CM Services software are provided in Table 3.2.2.4.1-1.

Table 3.2.2.4.1-1. Site and Configuration Audit Support Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.1-1	The system shall provide the capability to track audit schedules, agendas, facilities and rules of conduct as well as identify the participants.			
3.2.2.4.1-2	The system shall provide the capability to view and record hardware and software installed on remote DII COE-based systems.			
3.2.2.4.1-3	The system shall identify the tools and inspection equipment and test software necessary for evaluation and verification of CIs during PCAs.			
3.2.2.4.1-4	DII COE CM tools shall support site auditing activities and shall report results through the distributed architecture.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.1-5	The system shall provide the capability to maintain and report the status on a CM Configuration Audit Checklist of CM actions to be completed prior to each functional and physical configuration Audit for the system and each CI, as applicable.			
3.2.2.4.1-6	The CM Configuration Audit Checklist shall include the following information for each item listed: a. Event priority b. Event criticality to accomplishment of CM objectives c. Event planned start date d. Event planned end date e. Event actual start date f. Event actual end date d. Reason(s) for schedule changes e. Event completion status (expressed as a percentage, if applicable) f. Event dependencies g. Organization/ Point-of-Contact responsible for coordination and completion of the event h. Event schedule thresholds i. Activities, programs, releases, etc., impacted by changes to event schedule j. Overall impact of changes to event schedule.			

3.2.2.4.2 Documentation Library Requirements

Documentation library requirements for CM Services software are provided in Table 3.2.2.4.2-1.

Table 3.2.2.4.2-1. Documentation Library Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.2-1	The system shall maintain applicable specifications, drawings, schedules, verification test plans and procedures, verification test results, and documentation on demonstrations, inspections and analyses.			
3.2.2.4.2-2	The system shall maintain current deviations/waivers that impact existing baselines and identify CIs affected, how DII COE is impacted by the use of the deviation/waiver, the deviation/waiver effectivity date and expiration date, and the classification of the deviation/waiver (minor, major or critical).			
3.2.2.4.2-3	The system shall maintain an account of the approved ECPs incorporated and tested as well as proposed ECPs. The system shall identify CIs affected by the ECP(s), how DII COE CIs are impacted by the incorporation of the ECP(s), and the type (Class I or II) and classification of the ECP (Emergency, Urgent, or Routine).			
3.2.2.4.2-4	The system shall maintain engineering drawings and engineering drafting manuals to support physical configuration audits (PCAs), as well as identification of the specific item(s) (specific serial numbers) to be reviewed.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.2-5	For each CI subject to FCA/PCA, the system shall maintain the following reference information: a. Applicable CI product specifications b. A list delineating both approved and outstanding changes against the CI c. Complete shortage list d. Acceptance test procedures and associated test data e. Engineering drawing index including revision letters f. Operating and support manuals, including operators manuals, maintenance manuals, illustrated parts breakdown, programmer's manuals, diagnostic manuals, etc. g. Proposed DD Form 250, "Material Inspection and Receiving Report h. Approved nomenclature and nameplates i. VDDs, for software j. FCA/PCA minutes for each CI k. Findings/Status of Quality Assurance Porgrams l. Program parts selection list m. Interface design document for software			
3.2.2.4.2-6	For each item configuration subject to PCA, the system shall maintain the following reference information: a. Current approved issue of hardware development and software and interface requirements specifications to include approved SCNs and approved deviations/waivers b. Identification of all changes actually made during test c. Identification of all required changes not completed d. All configuration documentation required to identify the CI e. In manufacturing instructions, manufacturing instruction sheets or computer-aided manufacturing (CAM) data related to drawings and computer-aided design (CAD) presentations of specified parts identified by the Government.			
3.2.2.4.2-7	The system shall provide the capability to compare the DII COE's and mission application's suite of baselined documents to the suite of "as-built" documents.			
3.2.2.4.2-8	The system shall provide the capability to generate and output reports on the results of comparing the DII COE's and mission application's suite of baselined documents to the suite of "as-built" documents.			
3.2.2.4.2-9	The system shall provide the capability to coordinate reports on the results of the document library comparison with and forward the reports to the responsible organizations.			

3.2.2.4.3 Software Library (Segments / Data) Requirements

Software library requirements for CM Services software are provided in Table 3.2.2.4.3-1.

Table 3.2.2.4.3-1. Software Library (Segments / Data) Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.3-1	The system shall be able to maintain a listing of software segment CIs being kept in the DII COE software library.			
3.2.2.4.3-2	The system shall be able to compare the listing of software segments maintained in the software library to appropriate baselines and the license database for license compliance. The system shall be able to track and report on any discrepancies detected as a result of the comparisons.			
3.2.2.4.3-3	The results from comparing the listing of software segments maintained in the software library to appropriate baselines shall indicate whether system CIs are the current approved version, an incorrect version, or an unknown segment.			
3.2.2.4.3-4	The system shall provide the capability to compare the DII COE's and mission application's suite of baselined software, data and database segment libraries to the suite of "as-built" software, data, and database segment libraries.			
3.2.2.4.3-5	The system shall provide the capability to generate and output reports on the results of comparing the DII COE's and mission application's suite of baseline software, data and database segment libraries to the suite of "as-built" software, data, and database segment libraries.			
3.2.2.4.3-6	The system shall provide the capability to coordinate reports on the results of the software library comparison with and forward the reports to the responsible organizations.			

3.2.2.4.4 Build List (Per Platform) Requirements

Build list (per platform) requirements for CM Services software are provided in Table 3.2.2.4.4-1.

Table 3.2.2.4.4-1. Build List (Per Platform) Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.4-1	The system shall be able to extract segment information from a set of release tapes and compare that information against the appropriate build list. The system shall be able to generate, display and output a report that identifies the discrepancies between the release tapes and the appropriate approved build list.			
3.2.2.4.4-2	Configuration information collected from DII COE-based system workstations shall be able to be compared to the appropriate approved build list.			
3.2.2.4.4-3	If discrepancies are found while comparing workstation configuration information with the current approved build list, the system shall be able to generate, display and output a report that identifies the workstation(s) and the discrepancies.			
3.2.2.4.4-4	The system shall provide the capability to coordinate reports on the results of the software build list comparison with and forward the reports to the responsible organizations.			

3.2.2.4.5 Fielded Equipment - Identification of Performance Problems and Firmware Requirements

CM Services software requirements for identification of performance problems and firmware requirements for fielded equipment are provided in Table 3.2.2.4.5-1.

Table 3.2.2.4.5-1. Fielded Equipment - Identification of Performance Problems and Firmware Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.5-1	The system shall provide the capability to identify the fielded models of hardware platforms and their firmware revision levels.			
3.2.2.4.5-2	The system shall provide for the collection and tracking of problem reports related to hardware platform models and their firmware.			
3.2.2.4.5-3	The system shall provide the capability to perform trend analyses of reported hardware and firmware problems to identify quality control problems of the hardware and firmware platform vendor.			
3.2.2.4.5-4	The system shall provide the capability to forward reports on identified quality control problems to the hardware/firmware platform vendor as well as a request to the vendor to identify a corrective plan.			
3.2.2.4.5-5	The system shall be able to measure and track hardware and firmware performance, and compare measured performance against thresholds and performance requirements recorded in appropriate HWCI specifications maintained for DII COE.			MIL-STD-973, H.5.1.1.1
3.2.2.4.5-6	If discrepancies are found and/or thresholds are exceeded while comparing hardware/firmware performance specifications with current hardware/firmware performance, the system shall be able to generate, display and output a report that identifies the HWCI(s)/firmware configuration item(s) (FWCI(s)) and the discrepancies.			

3.2.2.4.6 License Use / Allocation Requirements

License use/allocation requirements for CM Services software are provided in Table 3.2.2.4.6-1.

Table 3.2.2.4.6-1. License Use / Allocation Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.6-1	The system shall be able to identify the negotiated software license agreement for each COTS application loaded on each platform.			
3.2.2.4.6-2	The system shall be able to track and report on the number of licenses allocated versus the actual “use” of the COTS software application for a site.			
3.2.2.4.6-3	The system shall be able to identify whether the software licenses for any COTS applications loaded on a platform have expired.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.6-4	The system shall provide the capability to determine whether the terms of a COTS license have been violated.			
3.2.2.4.6-5	The system shall provide the capability to transfer the responsibility of tracking the number of licenses allocated to each applicable intermediate or "using" organization. The system shall provide both manual and automated mechanisms for effecting the responsibility transfer.			

3.2.2.4.7 Distributions Made Last Quarter Requirements

TBD

3.2.2.4.8 Current Web Information Requirements

TBD

3.2.2.4.9 Functional Audit Test Report Results Requirements

Functional audit test report results requirements for CM Services software are provided in Table 3.2.2.4.9-1.

Table 3.2.2.4.9-1. Functional Audit Test Report Results Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.9-1	The system shall record and report the results of DII COE system functional configuration audits (FCAs) to include the status and final disposition of identified discrepancies and action items.			
3.2.2.4.9-2	The system shall maintain and provide a report format for a matrix for each CI identifying specification sections 3 and 4 requirements cross-referencing: a. Test plan, procedure and results for each requirement verified by test; b. Documented results of demonstrations, inspections, analyses verifying requirements.			
3.2.2.4.9-3	For each action item and discrepancy recorded during an FCA, the system shall be able to maintain the following information, as appropriate: a. CI(s) impacted b. Type of Audit c. Date of Audit d. Status of action item/discrepancy e. Organization/ Point-of-Contact responsible for taking action f. Description of action g. Assigned suspense date for action resolution h. Number of days since the audit i. Actual date action was completed/discrepancy was resolved.			
3.2.2.4.9-4	The system shall provide the capability to coordinate FCA reports with and forward audit reports to responsible organizations.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.9-5	The system shall maintain and report the minutes of prior FCAs.			

3.2.2.4.10 CI and System Requirement Cross-Reference Requirements

CI and system requirement cross-reference requirements for CM Services software are provided in Table 3.2.2.4.10-1.

Table 3.2.2.4.10-1. CI and System Requirement Cross-Reference Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.2-1	The system shall be able to identify the system requirements satisfied by each CI.			
3.2.2.4.2-2	The system shall be able to identify the test procedures designed to validate the requirements satisfied by each CI.			

3.2.2.4.11 Physical Audit Test Report Results Requirements

Physical Configuration Audit (PCA) test report results requirements for CM Services software are provided in Table 3.2.2.4.11-1.

Table 3.2.2.4.11-1. Physical Audit Test Report Results Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.11-1	The system shall record and report the results of DII COE system physical configuration audits (PCAs) to include the status and final disposition of identified discrepancies and action items.			
3.2.2.4.11-2	The system shall provide the capability to compare the as-designed configuration build list to the actual system configuration.			
3.2.2.4.11-3	For each action item and discrepancy recorded during a PCA, the system shall be able to maintain the following information, as appropriate: a. CI(s) impacted b. Type of Audit c. Date of Audit d. Status of action item/discrepancy e. Organization/ Point-of-Contact responsible for taking action f. Description of action g. Assigned suspense date for action resolution h. Number of days since the audit i. Actual date action was completed/discrepancy was resolved.			
3.2.2.4.11-4	The system shall provide the capability to coordinate PCA reports with and forward PCA reports to responsible organizations.			
3.2.2.4.11-5	The system shall maintain and report the minutes of prior PCAs.			

3.2.2.4.12 Risk Assessment of Build Requirements

Risk assessment of build requirements for CM Services software are provided in Table 3.2.2.4.12-1.

Table 3.2.2.4.12-1. Risk Assessment of Build Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.12-1	The system shall be able to identify the risks, their severity and associated probability that are determined to be associated with each deployed DII COE build.			
3.2.2.4.12-2	The system shall be able to identify the risk mitigation strategies being employed at a site, how these strategies reduce the risks identified, and the risk probability resulting from the use of the strategy.			
3.2.2.4.12-3	The system shall provide the capability to generate and output a Risk Assessment Report detailing the results of a risk assessment and the identified risk mitigation strategies.			
3.2.2.4.12-4	The system shall provide the capability to coordinate the Risk Assessment Report with and forward the report to the responsible organizations.			

3.2.2.4.13 Test Readiness Review Support Requirements

Test readiness review requirements for CM Services software are provided in Table 3.2.2.4.13-1.

Table 3.2.2.4.13-1. Test Readiness Review Support Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.13-1	The system shall store and maintain an Operational Test Readiness Review (OTRR) Checklist for each DII COE software release and shall be able to track the status of the items in the checklist as appropriate. (A sample check list is provided in Figure 3.2.2.4.13-1 of this document.)			
3.2.2.4.13-2	The system shall provide the capability to trace operational test procedure steps to the requirements/capabilities they verify. Critical system requirements and capabilities not covered by operational test procedures shall be identified.			
3.2.2.4.13-3	The system shall provide the capability to generate a test coverage matrix matching DII COE requirements/capabilities to test results from developmental testing, integration tests, compliance tests, etc., to determine whether any requirements/ capabilities were not tested or were incompletely tested to date.			
3.2.2.4.13-4	The system shall provide the capability to trace critical operational issues to critical system requirements to support Test Readiness Review activities.			
3.2.2.4.13-5	The system shall have the capability to identify any possible COTS licensing issues at the proposed OT site during the scheduled OT timeframe.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.13-6	Critical system operational issues, requirements and capabilities to be covered by operational test procedures shall include: a. System performance b. Interoperability (the degree to which the data are correctly exchanged and interpreted between systems) c. Usability (the effort required to learn the user interface with the software, to prepare input and to interpret output of software) d. Maintainability (the effort required to modify the software) e. Security (how well the software safeguards classified information and handles unauthorized attempts at system/data access).			

3.2.2.4.14 Configuration Audit Metrics Requirements

The requirements covered by this section address metrics designed to measure the efficiency of established configuration audit processes. Configuration audit metrics requirements for CM Services software are provided in Table 3.2.2.4.14-1. (See also Appendix B for overview of metrics management approach.)

Table 3.2.2.4.14-1. Configuration Audit Metrics Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.14-1	The system shall provide the capability for authorized users to generate formatted and ad hoc reports depicting the differences between the original plan and subsequent changes in event data tracked in the CM Configuration Audit Checklist.			
3.2.2.4.14-2	The system shall provide the capability generate Gantt Charts, graphs and formatted and ad hoc reports summarizing the number and type of configuration audits planned, held, and successfully completed (all actions). The system shall be able to summarize the number of action items remaining open per audit. The system shall also be able to identify the number of resolved and unresolved discrepancies per audit.			
3.2.2.4.14-3	The system shall provide the capability to determine the number of open action items and unresolved discrepancies that are past due according to assigned suspense dates per audit.			

OPERATIONAL TEST READINESS REVIEW (OTRR) CHECKLIST

1. **T&E History**

a. Does the system possess any known priority 1 or 2 problems that impact the OT so as to constitute a deficiency relative to a critical operational issue?

b. Have all priority 3 problems been documented, complete with appropriate impact analyses, relativ e to each problem's potential impact to the system's mission capability and ability to resolve the affected critical operational issues?

c. Has the system functionality to be operationally tested and evaluated been made available prior to the start of OT?

d. Has the system functionality to be operationally tested and evaluated been developmentally tested?

e. Have features required to support system level requirements and the system interfaces required to interoperate with external systems been certified to be functional?

f. Were the system features of item (e) certified in an operationally realistic environment against operational requirements?

g. Are software requirements and design stable?

h. Has sufficient depth and breadth of software and interface testing been performed?

2. **Safety.** Does the system or software have any safety limitations (operational limitations for test personnel) either inside or outside the required performance envelop? If so, what corrective action has been taken or planned? Has a security release been issued?

3. **Reliability, Availability, Maintainability.** Have failure definition/scoring criteria been established? Has software been identified as a potential source of failure?

4. **Configuration Management.**

a. Is a deficiency identification, tracking and reporting system in place to support t he monitoring of deficiency reports by the operational test agency?

b. Are all required COTS licenses in place and valid though the period scheduled for OT?

c. Has a software configuration management system with associated control procedures been put in place prior to the start of OT?

d. Has the version of software to be used in the operational test been baselined?

e. Will the operational test agency have complete access to the configuration management system during the operational test period?

f. Will pending software or firmware changes, if any, be completed prior to the start of OT?

g. Is a physical configuration audit of the software version to be fielded planned?

5. **Integrated Logistics Support.**

a. Supportability.

(1) Has the software maintaina bility evaluation been completed?

(2) Was the maintainability evaluation performed by the post deployment software support agent?

(3) Is the Computer Resources Life Cycle Management Plan current?

b. Training. Will the materials used to train testers reflect the proposed operational test software baseline? If not, are workarounds in training needed? Have workarounds been approved?

6. **Security.** Has system security certification occurred? When is security accreditation planned?

7. **Test Resources.** Are any unique facilities, equipment, or software instrumentation required and will they be available at the test site(s)?

Figure 3.2.2.4.13-1. Operational Test Readiness Review (OTRR) Checklist

3.3 CSCI External Interface Requirements

CSCI external interface requirements for CM Services software are provided in Table 3.3-1.

Table 3.3-1: CSCI External Interface Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.3-1	The user interface with the system shall be in accordance with the current version of the *Defense Information Infrastructure (DII) Common Operating Environment (COE) User Interface Specifications*,			
3.3-2	The CM Services system shall support interfaces to the DII Hot Line database (HRR System).			
3.3-3	The CM Services system shall support interfaces to the Release Control Panels.			
3.3-4	The CM Services system shall support interfaces to the Test Library.			
3.3-5	The CM Services system shall support interfaces to the site asset database.			
3.3-6	DAD shall provide the capability to exchange data with external systems and databases using industry standard protocols and standards (e.g., delimited ASCII export and import).			
3.3-7	DAD shall provide the capability to exchange data with the configuration management system of each of the DII Programs. See Section 3.6, Adaptation, for any specific requirements of each DII Program.			
3.3-8	DAD shall provide the capability to exchange data with the license management system of each of the DII Programs. See Section 3.6, Adaptation, for any specific requirements of each DII Program.			

3.3.1 Interface Identification and Diagrams

None.

3.3.2 Project-Unique Identifier of Interface

None.

3.3.2.1 Software Interfaces

The CM Services has dependencies on other functional areas of the DII COE. These areas include, but are not limited to, the following:

- Office Automation
- Online Help
- Data Access Services
- Presentation Services
- Web Server
- Message Processing
- Global Data Management Services
- Data Management Services
- Distributed Computing Services

· Operating System Services.

Software interface requirements for CM Services software are provided in Table 3.3.2.1-1.

Table 3.3.2.1-1. Software Interface Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.3.2.1-1	The CM Services applications shall provide standard Applications Programmer's Interfaces (APIs) to allow other non-CM applications to access CM application functionality where possible. The viability of APIs in COTS and GOTS will vary widely. DISA will strive to have 100% exposure of APIs in GOTS applications and best case in COTS applications.			
3.3.2.1-2	The CM Services software shall support services provided by COTS products that operate with the Operating System (i.e., Distributed Computing Environment (DCE), Informix, CORBA, etc.).			

3.3.2.2 Input / Output Devices

Input/output device requirements for CM Services software are provided in Table 3.3.2.2-1.

Table 3.3.2.2-1. Input / Output Device Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.3.2.2-1	The CM Services shall support the Recommended Standard 232 (RS-232) interface to external systems.			
3.3.2.2-2	The CM Services shall support external SCSI devices used for communications devices or other communications uses.			
3.3.2.2-3	The CM Services shall support Ethernet interfaces for local area networks.			
3.3.2.2-4	The CM Services shall support peripheral devices used for printing functions.			
3.3.2.2-5	The CM Services shall support peripheral devices used for plotting functions.			

3.3.2.3 Input/Output Interfaces

TBD

3.3.2.4 Interface Definition

TBD

3.4 CSCI Internal Interface Requirements

CSCI internal interface requirements for CM Se rvices software are provided in Table 3.4-1.

Table 3.4-1: CSCI Internal Interface Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.4.1-1	DAD shall provide the capability to manage internal relationships, including dependencies, among assets.			
3.4.1-1.1	DAD shall provide the capability to add internal relationships, including dependencies, among assets.			
3.4.1-1.2	DAD shall provide the capability to modify internal relationships, including dependencies, among assets.			
3.4.1-1.3	DAD shall provide the capability to delete internal relationships, including dependencies, among assets.			
3.4.1-2	DAD shall provide the capability to generate reports showing internal relationships, including dependencies, among assets.			
3.4.2-1	DAD shall provide the capability to manage links between different instances of a Library.			
3.4.2-1.1	DAD shall provide the capability to add links between different instances of a Library.			
3.4.2-1.2	DAD shall provide the capability to modify links between different instances of a Library.			
3.4.2-1.3	DAD shall provide the capability to delete links between different instances of a Library.			
3.4.2-2	DAD shall provide the capability to manage links between different Libraries.			
3.4.2-2.1	DAD shall provide the capability to add links between different Libraries.			
3.4.2-2.2	DAD shall provide the capability to modify links between different Libraries.			
3.4.2-2.3	DAD shall provide the capability to delete links between different Libraries.			
3.4.2-3	DAD shall provide the capability to manage interfaces between different Libraries.			
3.4.2-3.1	DAD shall provide the capability to add interfaces between different Libraries.			
3.4.2-3.2	DAD shall provide the capability to modify interfaces between different Libraries.			
3.4.2-3.3	DAD shall provide the capability to delete interfaces between different Libraries.			
3.4.2-4	DAD shall provide the capability for an authorized user to access DAD functions and services for any Library.			

3.5 CSCI Internal Data Requirements

CSCI internal data requirements for CM Services software are provided in Table 3.5-1.

Table 3.5-1. CSCI Internal Data Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.5.1-1	DAD shall provide the capability for identification of assets by class.			
3.5.1-2	DAD shall provide the capability for each class to be configured with attributes that contain metadata about the assets within that class.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.5.1-3	DAD shall provide the capability to develop a core set of classes to be used in all DAD Libraries, with each class including a core set of attributes. This is intended to ensure some minimal compatibility and interoperability across different DAD Libraries.			
3.5.1-3.1	DAD core classes shall include but not be limited to: Segment, Patch, License, Documentation.			
3.5.1-3.2	DAD core attributes of the class Segment shall include: Object ID (unique), Segment Name, Segment Prefix, Segment Version, Material Date, Platform/Operating System, DII Program System Release Number, COTS or GOTS, Asset Version Number, Description, Download File Size, Installed File Size, Life-Cycle Status, License Status, Documentation, Platform Restrictions, Dependencies, Special Instructions, Asset Site Locations, Download Links.			
3.5.1-3.3	DAD core attributes of the class Patch shall include: Object ID (unique), Patch Name, Version, Material Date, Platform/Operating System, DII Program System Release Number, Original Asset Name, Original Asset Version Number, Description, Download File Size, Installed File Size, Life-Cycle Status, Documentation, Platform Restrictions, Dependencies, Special Instructions, Asset Site Locations, Download Links.			
3.5.1-3.4	DAD core attributes of the class License shall include: Object ID (unique), License Name, Version, Material Date, Platform/Operating System, DII Program System Release Number, Original Asset Name, Original Asset Version Number, Description, File Size, Life-Cycle Status, Download Links.			
3.5.1-3.5	DAD core attributes of the class Documentation shall include: Object ID (unique), Document Name, Document Number, Description, Publication Date, Life-Cycle Status, Links To Related Assets, Download Links.			
3.5.1-4	DAD shall provide the capability for the core classes and their core attributes to be defined automatically during initial installation of DAD software on relevant server(s) for a new Library.			
3.5.1-5	DAD shall provide the capability to manage core classes within a Library.			
3.5.1-5.1	DAD shall provide the capability to create core classes within a Library.			
3.5.1-5.2	DAD shall provide the capability to modify core classes within a Library.			
3.5.1-5.3	DAD shall provide the capability to delete core classes within a Library.			
3.5.1-6	DAD shall provide the capability to manage non-core attributes within any class within that Library.			
3.5.1-6.1	DAD shall provide the capability to create non-core classes within a Library.			
3.5.1-6.2	DAD shall provide the capability to modify non-core classes within a Library.			
3.5.1-6.3	DAD shall provide the capability to delete non-core classes within a Library.			
3.5.1-7	DAD shall provide an attribute within each asset class that links to the relevant asset file, e.g. Uniform Resource Locator (URL).			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.5.2-1	DAD shall provide the capability to manage a hierarchical taxonomy of multiple collections and subcollections to be used in browsing and searching for assets.			
3.5.2-1.1	DAD shall provide the capability to create collections and subcollections.			
3.5.2-1.2	DAD shall provide the capability to modify collections and subcollections.			
3.5.2-1.3	DAD shall provide the capability to delete collections and subcollections.			
3.5.2-2	DAD shall provide the capability to manage assets in collections and sub-collections.			
3.5.2-2.1	DAD shall provide the capability to add assets to collections and subcollections.			
3.5.2-2.2	DAD shall provide the capability to delete assets from collections and subcollections.			
3.5.2-3	DAD shall provide the capability to store asset files on DAD file server(s) corresponding to the collection structure.			

See Paragraph 3.2.1.2, Database Architecture Requirements, for additional internal data requirements concerning database data relationships and schema.

3.6 Adaptation Requirements

No adaptation requirements have been identified.

3.7 Safety Requirements

Safety is the responsibility of the overall system into which t he segmented CM Services software is embedded. The CM Services software shall not interfere with, nor defeat the purpose of, safety functions implemented in the host system.

3.8 Security and Privacy Requirements

General security and privacy requirements for CM Services software are provided in Table 3.8-1.

Table 3.8-1. Security and Privacy Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.8-1	All users shall be required to identify themselves to the system before performing any other actions.			
3.8-2	The system shall provide means to report on user activities while using the system.			
3.8-3	The system shall automatically create audit logs.			
3.8-4	The system shall list in the audit log events such as user activation or use of security-related functions or user actions such as changing accounts, changing classification, data purging, system configuration changes, etc.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.8-5	The system shall list in the audit log alerts that have been generated in response to actions that triggered audit log activation.			
3.8-6	The Security Manager shall have the ability to print and archive data recorded in the audit log.			
3.8-7	The system shall provide the Security Administrator with the capability to create individual login accounts.			
3.8-8	The system shall provide the Security Administrator with the capability to create/modify database user accounts.			
3.8-9	The system shall provide the Security Administrator with the capability to assign read, write, and modify data permissions.			
3.8-10	The system shall provide the Security Administrator with the capability to create defined operator profiles, including granting database privileges as established by the Database Administrator (DBA).			
3.8-11	The system shall provide the Security Administrator with the capability to customize menus by operator profile.			
3.8-12	The system shall allow individual user's privileges to be customized depending on their duties.			
3.8-13	System login shall be initiated exclusively by the user.			
3.8-14	The system shall maintain a record of each logon and logoff attempt, including used ID, role and time.			
3.8-15	The MIS database server shall be located in a secure facility.			
3.8-16	The system shall not allow users to change MIS database values not relevant to their duties.			
3.8-17	The system shall allow only approved persons to access MIS database values.			
3.8-18	Users shall have unique accounts within the system MIS DBMS. Those accounts shall have only the database permissions needed for their work.			
3.8-19	The system shall allow for an overlapping hierarchy of user permission sets with access levels ranging from no access, to view-only of some/all data, through write access to a single screen/table, to complete access to all tables.			
3.8-20	A user's database permissions will only be active within the context of the current application and database session. In other words, when a user starts a database session through some application, that session will only be able to access the data objects appropriate to the application and the only active permissions on those objects will be those appropriate to that application's use of those objects.			
3.8-21	Access to the MIS shall be password protected.			
3.8-22	Classified information shall not be stored in the MIS. In instances where the description of a problem is itself classified, a reference to an external, secured hard copy will be stored in the database.			
3.8-23	The system shall protect data from unauthorized disclosure and modification.			
3.8-24	The system shall provide the capability to identify and authenticate system users.			

3.8.1 DAD Security and Privacy Requirements

DAD security and privacy requirements for CM Services software are provided in Table 3.8.1-1.

Table 3.8.1-1. DAD Security and Privacy Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.8.1-1	DAD shall be accreditable to operate at the Collateral, Secret, and Top Secret/Sensitive Compartmented Information. To accomplish this DAD shall be C2 compliant, i.e. shall provide at a minimum a C2 level of security protection IAW DoD Standard DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, December 1985.			
3.8.1-2	DAD shall conform to requirements of the DII COE Security Services SRS which supercede any other security requirements where there is any conflict.			
3.8.2-1	DAD shall provide security mechanisms that ensure only authorized users have access to DAD.			
3.8.2-2	DAD shall provide the capability for authorized user to change his/her own password.			
3.8.2-3	DAD shall store account passwords in encrypted format.			
3.8.4-1	DAD shall utilize NSA approved encryption tools.			
3.8.4-2	DAD shall utilize the Public Key Infrastructure (PKI) per relevant DOD and DISA guidance.			
3.8.5-1	DAD shall provide the capability to track user activity.			
3.8.5-1.1	DAD shall provide the capability to maintain audit logs for a Library.			
3.8.5-1.1.1	DAD shall maintain an audit log for each authorized user access including the date, time, and user-id.			
3.8.5-1.1.2	DAD shall maintain a audit log for each unauthorized user access attempt including the date, time, and (if available) user-id and IP number.			
3.8.5-1.1.3	DAD shall maintain a audit log for each asset accessed (i.e., access of metadata) including the date, time, user-id, and segmentname (or assetname).			
3.8.5-1.1.4	DAD shall maintain a audit log for each asset download attempt, including date, time, user-id and IP number if available, and segmentname (or assetname), and downloadsuccess.			
3.8.5-1.1.5	DAD shall maintain a audit log for each successful asset download, including date, time, user-id and IP number if available, and segmentname (or assetname), and downloadsuccess.			
3.8.5-1.1.6	DAD shall have the capability to log success or failure of download attempts.			
3.8.6-1	DAD shall be restricted for posting classified, budgetary, acquisition, proprietary, or arms information.			

3.9 CSCI Environment Requirements

CSCI environment requirements for CM Services software are provided in Table 3.9-1.

Table 3.9-1. CSCI Environment Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.9-1	DII COE CM tools shall support a heterogeneous, multi-platform client/server environment.			
3.9-2	DAD server software shall reside and function in COE compliant environments.			
3.9-3	DAD client software shall be available for, and reside and function in, the current operational versions of all COE environments.			
3.9-4	DAD client software shall be available for, and reside and function in, the current operational versions of all COE environments.			
3.9-5	DAD client software shall be available for, and reside and function in, the current operational versions of non-COE Microsoft Windows and NT environments.			
3.9-6	DAD client software shall be available for, and reside and function in, the current operational versions of the major non-COE Unix environments.			

3.10 Computer Resource Requirements

3.10.1 Computer Hardware Requirements

As described earlier, the DII COE is a foundation for a designer to build systems on. It is not a system by itself though each component of the DII COE (kernel, infrastructure support applications, and common support applications) does require a certain amount of hard disk space and random access memory (RAM) to operate with. The designer of a DII COE-compliant system must determine the combined hardware requirements of the operating system, the DII COE kernel, the DII COE infrastructure services and the DII COE common support applications segments, and their mission application segments that will be loaded onto a hardware platform. Only after a thorough examination of each of these software components can the hardware be properly sized.

The MIS server shall be capable of running on existing CFI computer assets. (CMIS SRS Rqmt # 3.10.1)

DAD computer hardware requirements are provided in Table 3.10.1-1.

Table 3.10.1-1. Computer Hardware Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.10.1-1	DAD shall provide sufficient server storage capacity to store all of the assets and their metadata for the DII programs identified in Section 3.0, each having three major releases stored concurrently. Specifically, COE is estimated to require 75 GB (25 GB each release).			
3.10.1-2	DAD shall provide sufficient server storage capacity to store and execute all relevant DAD software.			

3.10.2 Computer Hardware Resource Utilization Requirements

The DII COE kernel installation procedures identify how much hard disk space and RAM is required to run that version of the DII COE kernel for a specific operating system. These specifications, in conjunction with operating system specifications, should be used as the minimum essential starting point for the designer of a DII COE-compliant system.

3.10.3 Computer Software Requirements

The DII COE kernel installation proce dures identify the size of the kernel software in megabytes. Only the DII COE kernel is required on a workstation in order for the workstation to be considered DII COE-compliant. It is the responsibility of the designer of a DII COE-compliant system to decide which additional DII COE infrastructure services and common support applications segments will be loaded beside the mission applications. The DII COE-compliant CM Services applications are considered part of the infrastructure services layer of the DII COE.

The MIS shall use an Oracle 7.X database as its core data repository and shall communicate with clients via TCP/IP. (CMIS SRS Rqmt # 3.10.3)

DAD computer software requirements are provided in Table 3.10.3-1.

Table 3.10.3-1. Computer Software Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.10.3-1	DAD software shall be COE-compliant.			
3.10.3-2	DAD shall provide access to users for all DAD user activities through any COE-compliant web browser client software.			
3.10.3-3	DAD shall provide the capability to conduct all DAD administrative activities through any COE-compliant web browser client software, with the following exception(s): deposit into DAD the asset files from external disk, tape, or other media.			

3.10.4 Computer Communications Requirements

Computer communications requirements for CM Services software are provided in Table 3.10.4-1.

Table 3.10.4-1. Computer Communications Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.10.4-1	DAD shall be accessible by any authorized user with access to the NIPRNET/Internet (unclassified), SIPRNET (secret), and/or JWICS (TS/SI/TK/US Only).			
3.10.4-1.1	DAD shall be available on the NIPRNET/Internet (unclassified).			
3.10.4-1.2	DAD shall be available on the SIPRNET (secret).			
3.10.4-1.3	DAD shall be available on JWICS (TS/SI/TK/US Only).			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.10.4-2	DAD shall provide the capability for users without static IP addresses to access DAD.			
3.10.4-3	DAD shall provide the capability for users with static IP addresses to access DAD.			

3.11 Software Quality Factors

Software quality factors are applied differently to DAD tools based on their source, GOTS or COTS. The design of any GOTS DAD tools will be in line with the software quality factors identified in the software developer's contract or derived from a higher level specification. For COTS applications, software quality factors may be used as decision criteria for choosing one product over another for inclusion in the DII COE when there are two or more applications of equivalent functionality. Examples of software quality factors include reliability, maintainability, availability, flexibility, portability, reusability, testability, and usability. Another factor to consider is the source of COTS, manufacturer or reseller, and what technical support agreements exist for maintaining the products.

Software quality factors requirements for CM Services software with respect to DAD are provided in Table 3.11-1.

Table 3.11-1. Software Quality Factors Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.11-1	DAD shall be developed using applicable industry and DoD software engineering practices.			

3.12 Design and Implementation Constraints

Design and implementation constraints for CM Services software are provided in Table 3.12-1.

Table 3.12-1. Design and Implementation Constraints.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.12-1	DAD shall conform to US policies.			
3.12-2	DAD shall conform to DoD policies.			
3.12-3	DAD shall conform to the DoD Joint Technical Architecture (JTA).			
3.12-4	DAD shall conform to the I&RTS.			
3.12-5	DAD shall conform to U.S. regulations.			
3.12-6	DAD shall conform to DOD regulations.			
3.12-7	DAD shall be Y2K compliant IAW DOD standards.			

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.12-8	DAD software shall be COE compliant.			
3.12-8.1	COTS products shall be segmented in accordance with COE I&RTS level six.			
3.12-8.2	GOTS products shall be segmented in accordance with COE I&RTS level six.			
3.12-9	DAD shall provide capability to enforce export restrictions on relevant COTS software. (This may be accomplished procedurally using user group access to protected products.)			

3.12.1 Dependencies on Other Software

Many of the CM Services applications require a supporting Relational Data Base Management System (RDBMS) to maintain the application specific data. The RDBMSs currently supported by the DII COE Engineering Office are:

DII COE Version 3.2

Oracle 7.3.2.3	Solaris 2.5.1 and HP-UX 10.20
Sybase 10.2.2.4	Solaris 2.5.1 and HP-UX 10.20
Informix 7.12	Solaris 2.5.1
Informix 7.22	Solaris 2.5.1 and HP-UX 10.20
MicroSoft Access	NT 4.00

3.12.2 Supported Operating Systems

Segmented CM Services applications may support any or all of the following operating systems based on the documented requirements. Section 3.2 identifies which requirements are required against a particular DII COE supported operating system. Those operating systems that are currently supported by the DII COE Engineering Office are:

DII COE Version 3.2

Solaris 2.5.1
HP-UX 10.20
NT 4.00

3.12.3 Client/Server Environment

Segmented CM Services applications must operate in a distributed client/server computing environment. This does not preclude client and server applications from being loaded onto the same workstation.

3.13 Personnel-Related Requirements

Not applicable. Personnel-related requirements must be determined by the developers of the DII COE-compliant system in which the CM Services applications are embedded.

3.14 Training-Related Requirements

Training requirements must be determined by the developers of the DII COE-compliant system in which the CM Services applications are embedded. In almost all cases the CM Services requirements will be satisfied by COTS CM applications. The developers of the DII COE-compliant systems may choose to use commercial training since most vendors do offer classroom instruction on their applications. Training-related requirements associated with Electronic Asset Distribution are listed in Table 3.14-1.

Table 3.14-1. Training-Related Requirements.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.14-1	Users of the system shall not require any specialized training that cannot be made available in-house on an ad hoc basis. CM personnel will perform initial training on the use of the system. Afterwards, the majority of MIS new-user training will be done by personnel within the user's department. CM personnel will conduct training as required in support of future releases containing new features.			
3.14-2	The system shall identify resources for Computer Based Training (CBT), training videos, and self-help guides.			
3.14-3	The system shall incorporate on-line help.			
3.14-4	The system shall provide context-sensitive help files that provide operation-specific information for both system users and administrators.			

3.14.1 DAD Training-Related Requirements

DAD training-related requirements for CM Services software are provided in Table 3.14.1-1.

Table 3.14.1-1. Design and Implementation Constraints.

Rqmt ID Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.14.1-1	DAD shall provide DAD documentation.			
3.14.1-1.1	DAD shall be supported by a User Guide.			
3.14.1-1.2	DAD shall be supported by an on-line help function detailing all DAD user functionality.			
3.14.1-2	DAD shall provide DAD training.			
3.14.1-2.1	DAD shall provide on-line tutorial training.			

3.15 Logistics-Related Requirements

Any DII COE-compliant system must meet the logistics requirements as called out in the appropriate logistics plan for that community of interest.

3.16 Other Requirements

All segmented CM Services applications for use in a DII COE-compliant system will be in accordance with the DII COE I&RTS. Applications must achieve a Level 5 compliance or higher before they are considered fieldable.

3.17 Packaging Requirements

CM Services applications segments will be formatted in accordance with the I&RTS. This requires that the segments can be read and installed by the COEInstaller tool distributed as part of the DII COE kernel. This does not imply that a specific CM Services application, in segmented form, will be available for *all* supported operating systems of the DII COE. The DII COE Engineering Office only gives direction to developers to produce segmented products for use on the various operating systems for which there is a documented requirement.

The DISA Center for Integration (CFI) Configuration Management Division is the central distribution facility for DII COE segments. Segments are distributed to DISA-sponsored programs, DII COE Engineering Office developers, and to Service/Agency distribution centers (e.g., Air Force, Army, Department of Defense Intelligence Information System (DoDIIS), etc.). Service/Agency users and developers with Service/Agency distribution centers must go through their cognizant DII COE distribution Point-of-Contact and not the DISA CFI facility. Please consult the DII COE HomePage for up-to-date information on software availability and distribution.

3.18 Precedence and Criticality of Requirements

The precedence and criticality of system requirements is primarily determined by the Configuration Review and Control Board (CRCB). Each requirement is assigned a priority which is used to determine its precedence and criticality, which in turn is used to determine its build assignment for implementation. If a conflict arises between requirements assigned to a build, the CRCB will be tasked with making the final decision for resolving the conflict. If a conflict arises concerning requirement precedence between levels of configuration documentation, the order of precedence is always (1) functional configuration documentation, (2) allocated configuration documentation, (3) product configuration documentation.

SECTION 4. QUALIFICATION PROVISIONS

This section defines the qualification methods used to ensure that the functional requirements identified in Section 3.2 have been met. However, these functional requirements only identify how DII COE-compliant CM Services applications must behave. They do not address the level of compliance of the CM services application segments in accordance with the DII COE I&RTS. Segments must be at least Level 5 compliant before they can be considered fieldable. It would not be appropriate for segmented CM Services applications to be compared against Section 3.2 if the segments fail to obtain Level 5 compliance.

Those CM Services applications that are considered an integral part of the DII COE and fall under the direct control and supervision of the DII COE CM TWG are delivered to the DISA CFI for testing. Developers of these DII COE segmented applications are required to deliver documentation in accordance with the *Configuration Management Software and Documentation Delivery Requirements (DDR)* document. The DDR references a second document, the *Defense Information Infrastructure (DII) Common Operating Environment (COE) Developer Documentation Requirements (DDDR)*. Both the DDR and the DDDR documents specify a number of documents that all DII COE developers must submit unless the DII COE Engineering Office has granted waivers. Three of the required documents are the Software Test Plan (STP), the Software Test Description (STD), and the Software Test Report (STR). The STP document describes the types of tests required and provides traceability to the software requirements the segments satisfy. The STP identifies the test locations, describes the test environment, and provides details concerning resources required for testing. The STD document describes the test cases and acceptance criteria that will be used to test the software. It describes the test methods, tools, scenarios, and the pass/fail criteria for assessing the results of the testing. The STD shall provide all essential information relating to each test so that an independent test can duplicate the test results or verify the results obtained. The final document in the trio is the STR. The STR document provides a technical report with supporting documentation (package of materials) required to evaluate the results of the software tests described in the STD. The STR documents the results of all tests run against the software, identifies problems encountered during testing, and recommends solution to those problems. These three documents are crucial in determining which requirements the segments satisfy.

The segmented CM Services applications will be qualified through formal validation tests in comparison to the SRS Section 3.2 requirements. The Qualification Methods applied to the segmented software shall include Compliance Test (CT), Test (T), Demonstration (D), Analysis (A), and Inspection (I).

Compliance Test (CT): A qualification method that is carried out by testers at the DISA OSF for DII COE applications. Applications segments are examined using the eight levels of compliance identified in the I&RTS. Test data are collected and subsequently examined to determine the actual level of compliance for each segment tested in accordance with the DII COE I&RTS. The data and tester's recommendations of a pass/fail, based on Level 5 compliance, are formulated into a test report and sent to the DII COE Engineering Office for final evaluation.

Test (T): A qualification method that is carried out by operation of the item, component, interface, or some part of the computer software configuration item that relies on the collection and subsequent examination of data. The collection of the data can be done using instrumentation or other specialized test equipment. In most cases this type of testing refers to functional testing.

In the case of GOTS CM Services software, functional testing is performed at the location designated by the DII COE Engineering Office. This testing encompasses the full breadth and scope of the GOTS application and ensures it meets the design criteria. Functional testing of COTS software is treated differently. The only functional testing performed at the DISA OSF is to ensure the segmented application launches, runs, and closes gracefully. Functional testing of the commercially baselined product is left up to its global customer base.

Demonstration (D): A qualification method that is carried out by operation of the item, component, interface, or some part of the computer software configuration item that relies on observable functional operation not requiring the use of elaborate instrumentation, special test equipment, or subsequent analysis. Typically, this qualification method is one of the easiest to perform.

Analysis (A): A qualification method that is carried out by the processing of accumulated data. An example of accumulated data is the compilation of data obtained from other qualification methods. The processing of the accumulated data normally involves interpretations or extrapolations made from the test data results. After the reduction, interpretation, or extrapolation of test data results a decision can then be made of whether the requirement in question has been satisfied.

Inspection (I): A qualification method that is carried out by visual examination, physical manipulation, or measurement to verify that the requirements have been satisfied. This may involve the visual examination of code, documentation, etc.

Special qualification methods may also be applied to the item, component, interface, or some part of the computer software configuration item that require special tools, techniques, procedures, facilities, and acceptance limits beyond those identified above.

SECTION 5. REQUIREMENTS TRACEABILITY

This entire section will be maintained in a different documen t due to the sensitive nature of planned capabilities vice actual implementation. The few paragraphs in this SRS only serve as a placeholder and are used to point to the other document. The removal of Section 5 allows for unrestricted distribution and for open posting of the SRS on the DII COE HomePage or any other web site. The actual Section 5, Requirements Traceability, can be found in the *Requirements Traceability Matrix for the Configuration Management (CM) Services Software Requirements Specification of the Defense Information Infrastructure (DII), Common Operating Environment (COE), (current version)* document which is restricted. Only U.S. Government Agencies may request and receive the requirements traceability portion of the SRS.

5.1 Objectives of Traceability

Traceability, in the context of the DII COE, means that each of the requirements identified in section 3.2, *Configuration Management Services Capability Requirements*, of this document is associated with a segment or collection of segments that satisfies the requirement. The segments that satisfy the requirement may differ by the DII COE Version, the supported operating system, or both. The matrixes in section 5.2 will identify this level of detail.

5.2 Requirements Matrixes

As previously stated, the actual requirements matrix is maintained in a different document. The first few DII COE-compliant CM applications became available during the fielding of DII COE Version x.x. Several more applications are scheduled for initial delivery during 1998 and should be included in DII COE Version x.x. The first version of the *Requirements Traceability Matrix for the CM Services Software Requirements Specification of the Defense Information Infrastructure (DII), Common Operating Environment (COE), (current version)* document is expected in 1998. Please contact the CM TWG chairperson if more information is required.

This page intentionally left blank.

SECTION 6. NOTES

6.1 Acronyms

The acronyms used in this document are defined as follows:

3GL	Third-Generation Language (high-level programming language, such as PL/I, C, or Java)
4GL	Fourth-Generation Language (designed to be closer to natural language than a 3GL language)
5GL	Fifth-Generation Language (programming that uses a visual or graphical development interface to create source language)
A	Analysis (Qualification Method)
ACAT	Acquisition Category
ACWP	Actual Cost of Work Performed
Alloc	Allocation
ANSI	American National Standards Institute
AOG	Architecture Oversight Group
AOG-ES	Architecture Oversight Group - Executive Session
API	Application Program Interface
APIRM	Application Program Interface Reference Manual
ARS	Action Request System
BAC	Budget At Completion
BCWP	Budgeted Cost of Work Performed
BCWS	Budgeted Cost of Work Scheduled
C4I	Command, Control, Communications, Computers, and Intelligence
CAGE	Commercial And Government Entity
CBT	Computer-Based Training
CCB	Configuration Control Board
CDCA	Current Document Change Authority
CD ROM	Compact Disk-Read Only Memory
CDRL	Contract Data Requirements List
CE	Completion Efficiency
CFI	Center For Integration
CFR	Code of Federal Regulations
CI	Configuration Item
CM	Configuration Management
CM TWG	Configuration Management Technical Working Group

CMIS	Consolidated Management Information System
COE	Common Operating Environment
COP	Common Operational Picture
COTS	Commercial Off-The-Shelf
CPI	Cost Performance Index
CR	Change Request
CRCB	Configuration Review and Control Board
CSA	Configuration Status Accounting
CSCI	Computer Software Configuration Item
C/SCSC	Cost/Schedule Control Systems Criteria
.csv	Comma Delimited Format (file suffix)
CT	Compliance Test
CV	Cost Variance
D	Demonstration (Qualification Method)
DAD	Defense Information Infrastructure (DII) Asset Distribution
DBA	Database Administrator
DBDD	Database Design Description
DBMS	Database Management System
DCE	Distributed Computing Environment
DCN	Design Change Notice
DDDR	DII COE Developer Documentation Requirements
DDDS	Defense Data Dictionary System
DDM	Department of Defense (DoD) Data Model
DDR	Documentation Delivery Requirements
DEL	Defense Information Infrastructure (DII) Enterprise Licensing
DID	Data Item Description
DII	Defense Information Infrastructure
DISA	Defense Information System Agency
Dist.	Distribution
DMS	Defense Message System
Doc	Document
DoD	Department of Defense
DoDIIS	Department of Defense Intelligence Information System
DoDISS	Department of Defense Index of Specifications and Standards
DP	Design Progress (metric)
DT	Development Test
DTP	Detailed Test Plan
EA	Executive Agent
EAC	Estimate At Completion

ECP	Engineering Change Proposal
EIA	Electronic Industries Association
Email	Electronic Mail
.eps	Graphics file format
ES	Errata Sheet
Eval	Evaluation
FAR	Federal Acquisition Regulation
FCA	Functional Configuration Audit
FMS	Foreign Military Sales
FWCI	Firmware Configuration Item
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GFE	Government Furnished Equipment
GID	Group Identification
GIF	Graphics Interchange Format
GMC	Global Command and Control System (GCCS) Management Center
GOTS	Government Off-The-Shelf
GSKS	Government Supplied Kernel Software
GSAS	Global Status Accounting System
GSPR	Global System Problem Report
GTAC	Unknown
HP	Hewlett-Packard
HRR	DII Hotline Database
HTML	Hyper Text Markup Language
HTTP	Hyper text Transfer Protocol
HW	Hardware
HWCI	Hardware Configuration Item
I	Inspection (Qualification Method)
ICWG	Interface Control Working Group
ID	Identification
IDD	Interface Design Description
IEEE	Institute of Electrical and Electronics Engineers
Info	Information
INFOSEC	Information Security
IP	Installation Procedure
IPT	Integrated Product Team
IRS	Interface Requirements Specification

I&RTS	Integration and Runtime Specification
ISO	International Standards Organization
JIEO	Joint Interoperability and Engineering Organization
JPEG	Joint Photographic Experts Group
J-STD	Joint Standard
JTA	Joint Technical Architecture
JWICS	Joint Worldwide Intelligence Information System
KPC	Kernel Platform Certification
LAN	Local Area Network
LCCB	Local Configuration Control Board
Lic	License
MB	Megabyte
MCG&I	Mapping, Charting, Geodesy and Imagery Exploitation
Mgmt	Management
MHz	Megahertz
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MIS	Management Information System
MNS	Mission Need Statement
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
.mpx	MicroSoft Project file format
NIPRNET	Unclassified (but Sensitive) Internet Protocol Routing Network
NM	Network Management
NOR	Notice of Revision
NT	Windows New Technology
OASIS	Operations Support Facility (OSF) Acquisition of Site Information System
OCD	Operational Concept Description
ODBC	Open DataBase Connectivity
.OLE	Object Linking and Embedding (file format)
OPR	Office of Primary Responsibility
ORD	Operational Requirements Document
OS	Operating System
OSD	Office of the Secretary of Defense
OT	Operational Test

OTRR	Operational Test Readiness Review
PC	Personal Computer
PCA	Physical Configuration Audit
PCRB	Preliminary Configuration Review Board
PDF	Portable Document Format (Adobe Acrobat File)
PM	Programmer's Manual
PPP	Point to Point Protocol
PR	Problem Report
PROM	Programmable Read Only Memory
QA	Quality Assurance
Qtr	Quarter
RAM	Random Access Memory
RDBMS	Relational Database Management System
Ref	Reference
RPC	Remote Procedure Call
RS-232	Recommended Standard 232
.rtf	Rich Text Format
S	Design Stability (metric)
SAC	Schedule At Completion
SAM	System Administrator's Manual
SCN	Software Change Notice
SCR	System Change Request
SCSI	Small Computer System Interface
SDD	Software Design Description
SDF	Software Development File
Seg	Segment
SegName	Segment Name
SHADE	Shared Data Environment
SIPRNET	Secret Internet Protocol Routing Network
SLIP	Serial Line Internet Protocol
SLOC	Software Lines Of Code
Sol	Solaris Operating System
SPI	Schedule Performance Index
SPS	Software Product Specification
SQL	Structured Query Language
SRB	Segment Release Bulletin
SRS	Software Requirements Specification

SSC SD	Space and Naval Warfare Systems Command (SPAWAR) Systems Center, San Diego, CA
SSL	Secure Socket Layer
SSS	System/Subsystem Specification
STD	Software Test Description
STP	Software Test Plan
STR	Software Test Report
SV	Schedule Variance
SVD	Software Version Description
SW	Software
T	Test (Qualification Method)
TAFIM	Technical Architecture for Information Management
TAR	Transfer Archive
TBD	To Be Determined
TCPI	To-Complete Performance Index
TCP/IP	Transmission Control Protocol/Internet Protocol
TEMP	Test and Evaluation Master Plan
TEP	Test and Evaluation Plan
.tsv	Tab Separated Values (file format)
TWG	Technical Working Group
UDP	Universal Datagram Protocol
UFD	User's Functional Description
UID	User Identification
UM	User's Manual
URL	Uniform Resource Locator
VDD	Version Description Document
Y2K	Year 2000

6.2 List of Terms and Definitions

The following definitions and explanatory information are applicable for the purpose of this document.

Account Management - Involves managing user and administrator accounts for all Instances of a Library.

Assets - Software or data related items that are stored electronically and can be reused.

Asset Group - A set of assets.

Asset Manager - The person with authority to release any of a set of a DII Program's electronic assets for distribution to authorized users. The Asset Manager is the Chief Engineer or Program Manager of that DII Program. For example, the DII COE Program has a Chief Engineer who is the Asset Manager. An Asset Manager delegates many DAD management activities including Library Management and Account Management.

Attribute - Elements of metadata which when used together identifies a unique product or asset available to a end-user.

Browser - An electronic tool that allows the end-user to view available collections or classes of assets.

Browsing - The act of navigating through hierarchies of classes and/or collections.

Class - A set of assets with identical or similar metadata formats, such as, software segments, software segment patches, database segments, guidance, documentation, and tools. A class, to be adequately described, needs attributes different from other classes. In other words a class is like a database table, an attribute is like a field in that table, and an asset's metadata becomes a record in that table. Examples of some possible classes are: segments, segment documentation, and license terms and conditions.

Class Hierarchy - The logical arrangement of classes and subclasses to facilitate search and location of a unique asset.

Collection - A set or inventory of assets of various classes under the control of a Asset manager's configuration management. For example, the COE Library contains a collection of assets of a particular COE version, and within that COE version are sub-collections corresponding to Kernal, Infrastructure Services, and Common Support Applications. A group of assets that share a common subject, theme, or content. Collections are presented hierarchically to further indicate relationships between collections by displaying subcollections as indented beneath parent collections. Collections can contain assets of more than one class.

Collection Hierarchy - The logical arrangement of collections and sub-collections to facilitate finding a unique asset. A taxonomy. An administrative hierarchy of relationships between collections.

Configuration Management (CM) - CM is one of the five major MFAs that is described in the ISO OSI Management Framework and System Management Overview standards. The CM MFA defines requirements to determine/monitor (via interrogation, polling or event -driven reporting), to detect changes in, and to control the arrangement, relationships, characteristics and state (for example, initialize/terminate, activate/deactivate, idle/busy, etc.) of individual and specifiable aggregates of managed resources so as to maintain continuous operation and/or delivery of

service. CM as used in this document is not to be confused with CM as used in MIL-STD-483 (Configuration Management Practices for Systems, Equipment, Munitions, and Computer Programs) or MIL-STD-1456 (Configuration *Management Plan*).

Databases - Databases are archival repositories persistently stored on electro/optical media. Databases are accessed or updated by database management systems. Databases are generally used by, and shared among, manager systems by means of standard database query languages, such as SQL and RDA. Some databases may be integrated across several different manager systems and/or management domains.

Enumeration - A list of special values used as an attribute data type.

Instance - A fully functional copy of a Library; for example the COE Library may have 3 instances on different networks of different security classifications.

Interoperability - (1) The ability of two or more systems to exchange and use information. (2) Application software operating on heterogeneous hardware/software platforms that cooperates in performing a user task and sharing data.

JWICS - The Joint Worldwide Intelligence and Communications System, a Top Secret network.

Library Management - Involves managing all of a Library's assets and related metadata in all Instances of that Library.

Library - A defined set of collections of assets. In this document Library is used to indicate all of the assets of a particular DII Program or Asset Manager.

Metadata - An information set that provides a complete description of an asset.

Natural Language Search - A search that uses natural language search criteria.

NIPRNET - The Not Classified Internet Protocol Router Network is a DOD unclassified network provided by DISA.

Portability - (1) The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to significantly modify the application being transported. (2) The ability of software or of a system to run on more than one type or size of computer or under more than one operating system. (3) Synonymous with transportability. How easy or difficult it is to move an application between computer platforms and retain functionality with minimal change or conversion of the software.

Scalability - The ability to use the same application and system software vertically across hardware platforms, from desktop workstation to large mainframes, to match the needs of a given user community.

Segment - A collection of one or more software and/or data units most conveniently managed as a unit of functionality. Segments are defined from the perspective of an operator, not a developer, and are generally defined to keep related units together so that functionality may be easily included or excluded. They are usually defined as functional pieces (e.g., a word processor) that make sense from a system administrator perspective because segments are the lowest level components that can be installed on, or removed from, a platform.

Server Management - Involves managing the physical server(s) upon which a portion of DAD resides, general system administration of the server(s), and security for the server(s).

Single Sign On - A single strong identification and authentication (I&A) process that can reliably be used for access control by any receiving process, whether or not it is within the same security domain. The process can determine the user's rights and permissions and make (immediate and subsequent) access control decisions to the process resources without further I&A exchanges with the user. Also known as Unitary Login.

SIPRNET - Secret Internet Protocol Router Network, the DOD network at Secret classification provided by DISA.

System - A system is a set of information processing and data processing resources (such as computers), together with any supporting system software (such as operating systems and DBMSs), any peripheral devices, any supported applications and files, and any communications infrastructure that interconnects the system's components, end -users of such system resources, and the users and components of other systems. A system is generally considered to include all hardware and software components, facilities, personnel, and procedures that are necessary to support applications.

Tier Management - Involves an Asset Manager's customer organizations, each with authority to manage further distribution, into one or more lower levels of distribution. There may be any number of Tiers between a Library and a User. The specifics for use of Tiers are the result of agreement between the Asset Manager and his/her customers. DAD is envisioned to have capability to distribute to first level tiers of each Service or Agency organization, for further distribution, or to distribute directly from Library to end user.

User Group - A membership set of users. User groups can be members of other user groups.

This page intentionally left blank.

APPENDIX A: MANAGEMENT INFORMATION SYSTEM (MIS) STYLE GUIDE

(From CMIS SRS, Appendix A)

A.1 Style Guide

The guidelines listed below will be applied to all new products developed as part of the MIS. They are to be used as guidelines, there will certainly be instances where following them would not be appropriate. In those cases, the choice will be at the discretion of the designer and/or primary user. In porting legacy products, consideration will be given to maintaining a similar look and feel even when such design conflicts with these guidelines.

A.1.1 Forms Standards

a. All x-y coordinates and sizes specified in this document are based on the following Ruler settings: - From the Layout Editor, select **V**iew > Setting**s** > Rule**r**... and set the parameters as follows:

Units			Points.
Character Cell Size (points)	Horizontal		6
Character Cell Size (points)	Vertical		16
Grid Spacing	Other		12
Number of Snap Points Per Grid Spacing			2

b. Window Frame.

1. All window frames should be initially set to 474 x 289. This allows the best fit to a 13" monitor @ 640 x 480 resolution.
2. A short title should be supplied that is both unique to this form and descriptive of the form function.

c. Canvas Views.

1. As much as is practical, canvas views should be limited to as much information as can be comfortably displayed in the standard window frame described above.
2. Where larger canvasses are necessary, consideration should be given to the following:
3. For a spread table type of display:
    a. Additional columns should be displayed to the right, with the most important/most used data elements displayed left-most.
    b. Key elements should appear first and be locked to the content canvas, with all other elements displayed on a stacked canvas and scrollable by a horizontal scroll bar located immediately below the display area. Scroll bar width should match the display area, and height should be 12 points.
    c. A vertical scroll bar should be included and fixed to the content canvas. It may be located either left or right of the data display, but should match the display area in height Scroll bar width should be 12 points.
4. For individual item or combination canvasses that extend vertically beyond the window frame, a vertical scroll bar should be affixed to the window frame.

5. For individual item or combination canvasses that extend vertically and horizontally beyond the window frame, both vertical and horizontal scroll bars should be affixed to the window frame.

d. Colors, Fonts, and Alignment. For phase one, to keep things simple, all canvasses should have the following characteristics:

1. Colors:

   a. Canvas background — Gray
   b. Canvas boilerplate — Black
   c. Data element background — White
   d. Data element text — Black

2. Fonts and Sizes:

   a. Canvas headers:

      1. New Times Roman font
      2. Up to 14 point pitch
      3. Bold
      4. Underlined, if desired

   b. Boilerplate text (data item labels, column headers, etc.)

      1. New Times Roman font
      2. 10 point pitch
      3. Bold

   c. Text data display:

      1. Height — 18 points max, 16 points min
      2. Width — sufficient for adequate data display.
      3. Space between records — 0 for spread table display; As required for all others.

3. Bevel — Lowered
4. Rendered — True
5. Font name — <none>
6. Font size — 10 max, 8 min (dependent on height, above)
7. Font style — Plain
8. Font width — Normal
9. Font weight — Medium (10 pitch), bold (8 pitch)
10. Date format:

    a. date-only data elements — DD Mon YYYY
    b. date/time data elements — DD Mon YYYY HH24:MI
       mm/dd/yyyy (CM Library functions only)

11. List boxes: Should only be used when domain of values is small and static. (Dynamic domains of values should be accessed by LOV.) Font and size considerations should be the same as text data.

12. Alignment:

    a. Spread format:

        1. Vertically align top
        2. Horizontally stack

    b. Non-spread format: Grouped data elements should be aligned/stacked as necessary to present a consistent, "finished" appearance to the form. While this is a very subjective area, organization and appearance of data elements are important to user acceptance.

e. Button palette.

1. Content:

    a. Each form shall have a prominently displayed exit button.

    b. For forms that will be used primarily for query, enter query/execute query, scroll up, scroll down, previous record, and next record buttons shall be added to the above.

    c. For forms that will also be used for maintenance of data, insert, delete, and save buttons shall be added to the above as appropriate.

    d. For forms from which the user will have the ability to generate a predefined report, a print button shall be added to the above as appropriate.

    e. For forms that will be used for data entry/data maintenance, a button shall be provided to initiate List of Values display in order to aid the user in selecting only valid values. This button should be located immediately adjacent to the data element to which it applies. A button 12 points in width, with a height matching the data element to which it applies, and a '?' for a label is recommended.

2. Characteristics:

    a. width 48 points
    b. height 16 points
    c. font (labels) 10 point plain text (Recommend 'EXIT' be all caps)
    d. alignment: vertically align top
       horizontally stack

3. Placement: The button palette shall be placed at the bottom of the window frame, where practical, or alternatively, the bottom of the primary content canvas.

4. Sequence.

    a. Scroll up
    b. Previous record
    c. Next record
    d. Scroll down
    e. Enter/execute query
    f. Insert
    g. Delete
    h. Save

i. Cancel/Exit

5. Usage:

a. When in enter-query mode:

1. The label of the query button should read 'Execute', and the when-button-pressed trigger should execute the query.
2. The label of the exit button should read 'Cancel'.
3. All other buttons should be disabled.

b. When in normal mode:

1. The label of the query button should read 'Query', and the when-button-pressed trigger should place the form in enter-query mode.
2. The label of the exit button should read 'EXIT'.

c. All other buttons should be enabled as appropriate.

f. Scroll bars.

1. Vertical

a. Width 12 points
b. Height match the height of t he display area to which the scroll bar applies
c. Placement Place the scroll bar immediately adjacent to the display area to which it applies, as in a stacked alignment. Whenever practical, the vertical scroll bar should be placed at the right edge of the data display area.

2. Horizontal

a. Width match the width of the display area to which the scroll bar applies
b. Height 12 points
c. Placement Place the scroll bar immediately below the display area to which it applies, as in a stacked alignment.

g. Cursor.

1. When initiating any function that will likely cause a discernible delay to the user, set the cursor attribute to busy as follows:

set_application_property (cursor_style,'BUSY');

2. When the function is complete, reset the cursor attribute as follows:

set_application_property(cursor_style,'DEFAULT');

3. This should be accomplished as follows:

a. When invoking another form.

1. The command sequence to invoke the new form should set the cursor attribute to busy as its first act.
2. The new form should reset the cursor attribute as its last startup act. (This is usually accomplished in a when-new-form-instance trigger.)

b. When initiating a run_product command, as in generating a predefined report.

1. The command sequence in which the run_product command appears should set the cursor attribute to busy as its first act.
2. The command sequence in which the run_product command appears should reset the cursor attribute as its last act

c. When initiating any process that will likely cause a discernible delay in system response to the user.

1. The command sequence in which the process is initiated should set the cursor attribute to busy as its first act.
2. The command sequence in which the process is initiated should reset the cursor attribute as its last act.

A.1.2 Process Standards

a. Delete records. Extreme caution should be exercised in allowing record deletion. By default, ALL blocks with a base table should have delete allowed set to false.

1. For data maintenance forms where record deletion is desirable, a test should be made in the when-new-form-instance trigger for user privilege level. If the user has sufficient privilege, turn delete allowed on for the appropriate block(s).
2. If there is a potential dependency between the record to be deleted and one or more records in one or more tables, and no database constraint exists to enforce the relationship, code **MUST** be invoked to prevent the deletion until the dependency is appropriately removed.
3. If the record deletion is valid according to the above criteria, an alert box should be displayed to verify that the user actually does wish to delete the selected record.
4. The alert box should have the following characteristics:

- Title	Delete Check
- Alert style	Caution
- Button 1	OK
- Button 2	Cancel
- Default alert button	Button2
- Message	Do you really want to delete this record?

5. All other properties as defaulted.

b. Insert records. By default, ALL blocks with a base table should have insert allowed set to false.

1. For data maintenance forms where record insertion is desirable, a test should be made in the when-new-form-instance trigger for user privilege level. If the user has sufficient privilege, turn insert allowed on for the appropriate block(s).

c. Update records. By default, ALL blocks with a base table should have update allowed set to false.

1. For data maintenance forms where record updating is desirable, a test should be made in the when-new-form-instance trigger for user privilege level. If the user has sufficient privilege, turn insert allowed on for the appropriate block(s).

2. By default, ALL columns within an updatable block should have insert allowed and update allowed turned off. Additional code should be entered in the when-new-form-instance trigger so that, upon validation as an update-capable user, only those fields appropriate for update will have update allowed turned on.

A.1.3 Reports Standards

a. Parameter Screens

1. Whenever the format of a report calls for Landscape mode printing, the message "*** This is a Landscape report ***" will be prominently displayed on the Report Parameter form to give the user notice to set the printer properly.
2. Report Destination Type on the Report Parameter form will be defaulted to 'Preview'.
3. Report Parameter forms will be sized so that all fields can be seen without the user's having to scroll down.

b. Report Formatting

1. Any report of more than 2 pages will have a header page.
2. All reports that can potentially retrieve more than one record will have the selection criteria that specified the report included, either on the header page or before the first data record.
3. All reports will have an end-of data indicator, either a bold and/or negatived final line or a trailer page.
4. All reports will have 'For Official Use Only' prominently displayed on the cover page or as a banner line on data pages.

APPENDIX B: METRICS OVERVIEW

This appendix provides an overview of some of the metrics specified in this SRS for measuring process efficiency of DII COE configuration management and control functions and software product quality. A summary description is provided for each type of metric addressed, as well as guidance for implementing the metrics as part of the automated CM Services software system. The metrics were selected based on their applicability to DII COE CM functions and processes and their capability to provide DII COE program managers with the insight needed to make informed decisions on software management issues.

DoD 5000-2R requires software metrics be used on all acquisition category (ACAT) I, IA and DoD oversight systems. Metrics to be included in CM Services Software will provide indicators for evaluating cost, schedule, requirements traceability, and fault profile status and trends. The metrics requirements in this SRS also specify capabilities for tracking the information and collecting the data items needed for the metrics described. DoD policy also requires applicable systems to demonstrate, prior to entering dedicated operational testing, that design is stable and that adequate testing of software and interfaces has occurred. The design stability and breadth of testing metrics described in the requirements in Sections 3.2.2.1.12, 3.2.2.2.16, 3.2.2.3.8, and 3.2.2.4.13 are designed to support this policy.

The metrics described fall into six general categories as shown in Figure B-1. Management metrics address programmatic and over all management issues. COTS licensing metrics address license requirements and distribution. Requirements metrics pertain to the specification and traceability of existing requirements and the processing of new requirements. Change management metrics pertain to CM processes for handling ECPs. Asset submission/distribution metrics address how assets are submitted and distributed, electronically or manually. Quality metrics address testing, thresholds, GSPRs and other technical characteristics of software products. For each metric identified, data items collected must be consistently defined and calculated to give an accurate and meaningful representation of overall program health.

B.1 Cost Metric

The cost metric indicates how well software development and life cycle costs are controlled. The cost metric compares actual cost expenditures for software development tasks to initial cost estimates. Data for the cost metrics are selected from the cost accounting system used for most DoD acquisition programs, the Cost/Schedule Control Systems Criteria (C/SCSC). The first step in applying the software cost metric is to identify the appropriate software work tasks, or activities, as cost elements. The activities identified must allow software costs to be accountable to individual DII COE computer software configuration items (CSCIs), builds, and subsystems to provide the level of visibility needed to monitor risk effectively. The contractor's accounting systems provide accumulation of actual cost of accomplished work, that is compared with earned value, providing a cost variance for the accomplished work and indicating whether the work is over, or underrunning its plan.

Metric	Objective	Measurement
Management Metrics		
Cost	Track planned and actual S/W expenditures	$ spent versus $ allocated
Schedule	Track schedule adherence	Milestone/event slippage
Manpower	Track staff requirements, allocations, and levels of effort	Measures the planned level of effort, the actual level of effort, and the losses in staff
COTS Licensing Metrics		
COTS License Management	Track license requirements and distribution	# licenses required/purchased/ distributed
Requirements Metrics		
Requirements traceability	Track requirements to code and test cases	% requirements traced
New Requirements	Track time for processing new requirements	New requirement processing time
Requirements Change	Track amount of requirements changing	% requirements changed
Change Management Metrics		
Change Requests/ Proposals	Track ECP Cycle times	ECP processing time
ECP Approval Rate	Track rate of ECP approval upon 1st review by CCB	% Approved upon 1st review by CCB
Quality Gate Task Status	Track status of tasks during the current reporting period	# of tasks due, completed on time, completed late, and overdue
CM Churn Per Month	Tracks number of baselined CIs that have been modified and resubmitted	% of baselined CIs changed during the month
Asset Submission/Distribution Metrics		
Segment Submissions	Track how segments and documentation are submitted (electronically vs. manually)	# segments submitted electronically/manually
Asset Distribution	Track how assets are being distributed	# assets distributed electronically/manually
Quality Metrics		
Design Stability	Track design changes	Stability index
Breadth of Testing	Track testing of requirements	% requirements tested and % requirements passed
System Thresholds	Track threshold violations	# and types of threshold violations
Fault Profiles	Track open versus closed anomalies	# and types of faults
Deviation Profiles	Track deviation requests and usage	# of deviations requested/approved; # of each type of deviation

Figure B-1. CM Services Metrics

Many of the requirements for cost and schedule metrics cited in this SRS are derived from the Project Control Panel gauges described in *The Program Manager's Guide to Software Acquisition Best Practices*, October 1997 (Chapter 2). The Project Control Panel Gauge is shown in Figure B-2. The data items to be collected for cost and schedule metrics based on the Project Control Panel gauges are described below.

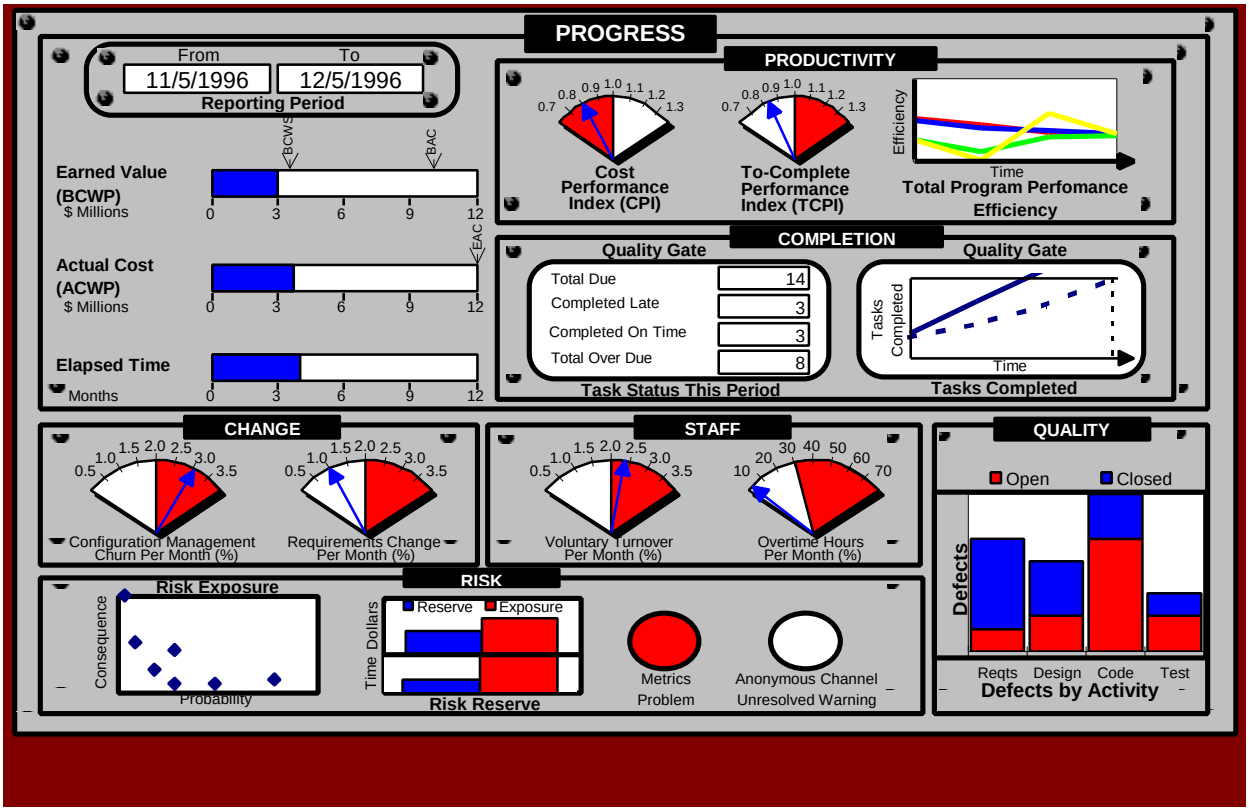

Figure B-2. Project Control Panel

(1) Budgeted Cost for Work Performed (BCWP) (also called **Earned Value**) represents the sum of the budgets for completed work tasks/packages and completed portions of open work tasks/packages, plus the applicable portion of the budgets for level of effort and apportioned effort (reflects actual progress made toward completing the planned work). [NOTE: *Establishing a planned value and a completion criterion for each task before work begins is critical for using the Earned Value metric successfully to measure progress.*]

BCWP = (% of tasks completed) X (planned cost for each task)

(2) Budgeted Cost of Work Scheduled (BCWS) represents the sum of the budgets for all work tasks/packages scheduled to be accomplished (including in-process and completed work tasks), plus the level of effort and apportioned effort scheduled to be accomplished within a given time period.

(3) Budget At Completion (BAC) represents the sum of all budgets allocated for the release or contract. This is usually the contract target or estimated cost, plus authorized, unpriced work.

(4) Actual Cost of Work Performed (ACWP) represents the actual costs incurred and recorded in accomplishing the work performed within a given time period. By comparing ACWP with BCWP, a manager can estimate how the project is performing against its budget.

ACWP = sum of the actual cost of the tasks performed

(5) Schedule At Completion (SAC) is the original scheduled completion date. Current time can be compared with SAC to determine the time remaining in the original schedule.

(6) Schedule Performance Index (SPI) measures the degree to which program events adhere to a work schedule plan. Values less than one indicate the schedule is exceeding estimates.

SPI = BCWP / BCWS

(7) Completion Efficiency (CE) estimates the productivity required to complete the release within a projected total cost (EAC).

CE = BAC / EAC

(8) Estimated Cost at Completion (EAC) is the actual direct costs and indirect costs allocable to the contract, plus estimate of costs (direct and indirect) for authorized work remaining. It is the latest revised estimate of the value of remaining work plus actual costs to-date.

EAC = ACWP + estimated cost of remaining work

(9) Cost Performance Index (CPI) measures the relationship between the value (planned cost) of the work accomplished and how much it actually cost to do that work. Values less than one indicate the cost is exceeding estimates and a potential productivity problem exists, or that the original budget was too aggressive for the amount of work to be performed.

CPI = BCWP / ACWP

(10) To-Complete Performance Index (TCPI) indicates cost performance efficiency (i.e., average productivity) required to accomplish the remaining work within the BAC. It is calculated by dividing the work remaining by the current estimate of remaining cost.

TCPI = (BAC - BCWP) / (EAC - ACWP)

By applying cost metrics, the degree that actual cost values (i.e., ACWP) correspond to their original planned values (i.e., BCWS and BCWP) can be analyzed by plotting cost data over time. A sample cumulative cost graph is provided in Figure B-3. Other cost values and indicators can be similarly plotted over time to identify potential problems areas and risks to the overall program. Cost performance is determined by calculating cost variance (CV), the difference between planned and actual cost (CV=BCWP-ACWP). Exceeding budgeted allocations is detected by a negative value for CV. Consistently or increasing negative values for CV indicates the system may exceed the budget.

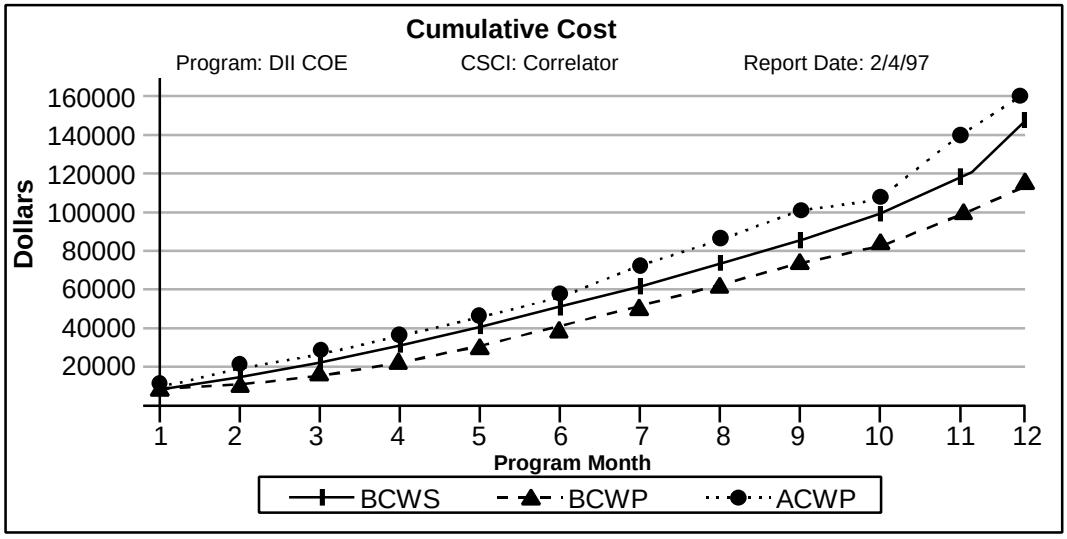

Figure B-3. Sample Cost Expenditure Graph

B.2 Schedule Metric

The schedule metric indicates changes and adherence to planned schedules for major system development milestones, activities and key software deliverables. Monitoring schedule changes will indicate the level of risk associated with achieving future program milestones and providing key software deliverables on time. Maintaining the original end dates in a schedule after early delays usually requires additional resources.

The schedule metric can be used in conjunction with other metrics to assess program risk. The fault profiles and development progress metrics provide information about the amount of work that remains to be done. The cost metric indicates if resources are available to accelerate the work rate and meet the original schedule. The cost and schedule metrics together can be the best early indicators of problem areas, allowing managers to focus attention in these areas and resolve problems before they get out of hand.

The degree that actual event timelines correspond to their original planned schedule can be calculated by plotting schedule data over time. One recommended display of schedule data is a graph of planned start dates for program milestones and key software deliverables over time, as shown in Figure B-4. Planned start dates for an event are plotted until the event actually begins (i.e., an actual start date has been reported). In this example, the planned start dates for several software development activities are plotted over the month in which the data was reported. The graph shows the compression of time between the start of software requirements analysis and design. To read the graph, find the metric reporting date (program month) on the x-axis, and read the appropriate planned start date on the y-axis. For example, at month one, requirements analysis was planned to start in month two, and the software design was planned to start in month eight. At month two, the start of requirements analysis has slipped to month three (a slip of one month), but the start of software design has remained the same. At month five, the start of requirements analysis has slipped to month six (a total slip of four months), and the software design schedule has only slipped one month.

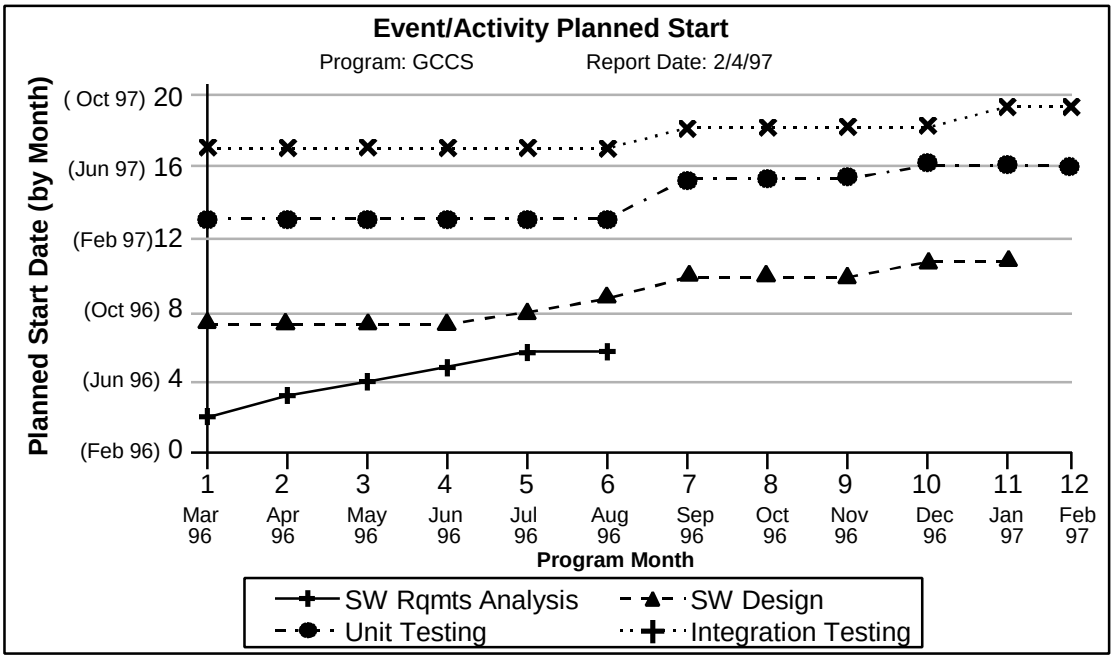

Figure B-4. Sample Schedule Metric Graph

Another metric for assessing schedule performance is determined by calculating schedule variance (SV), the difference between the amount of work planned to be performed and actually completed (SV=BCWP-BCWS). Consistently or increasing negative values for SV indicates the system may be delivered behind schedule.

B.3 Manpower Metric

The manpower metric provides an indication of the application of human resources to the project, both developer and Government, and the ability to maintain sufficient staffing to complete the project. The manpower metric is composed of two parts: an effort measure monitors labor hours planned and expended, while a staffing measure accounts for quantity and types of personnel needed to do the work. This metric assists in determining whether the developers and the Government have scheduled a sufficient number of employees to produce the product in the time and budget allotted. To derive the manpower metrics, for each CSCI, labor category, and experience level track:

1. Labor category
2. Experience level (experienced, special, total)
3. Number of personnel planned to be on staff for the reporting period.
4. Number of personnel actually on staff in the reporting period
5. Number of unplanned losses in personnel that occurred
6. Number of labor hours planned to be expended in the reporting period (cumulative)
7. Number of labor hours actually expended in the reporting period (cumulative).

The primary information obtai ned from the manpower metric is derived by comparing planned and actual levels of effort and personnel. Figure B-5 depicts the effort measure for an entire system for all labor categories over time. Figure B-6 is an example of a staffing profile. Displays can be organized by CSCI or individual labor category for more detailed analysis.

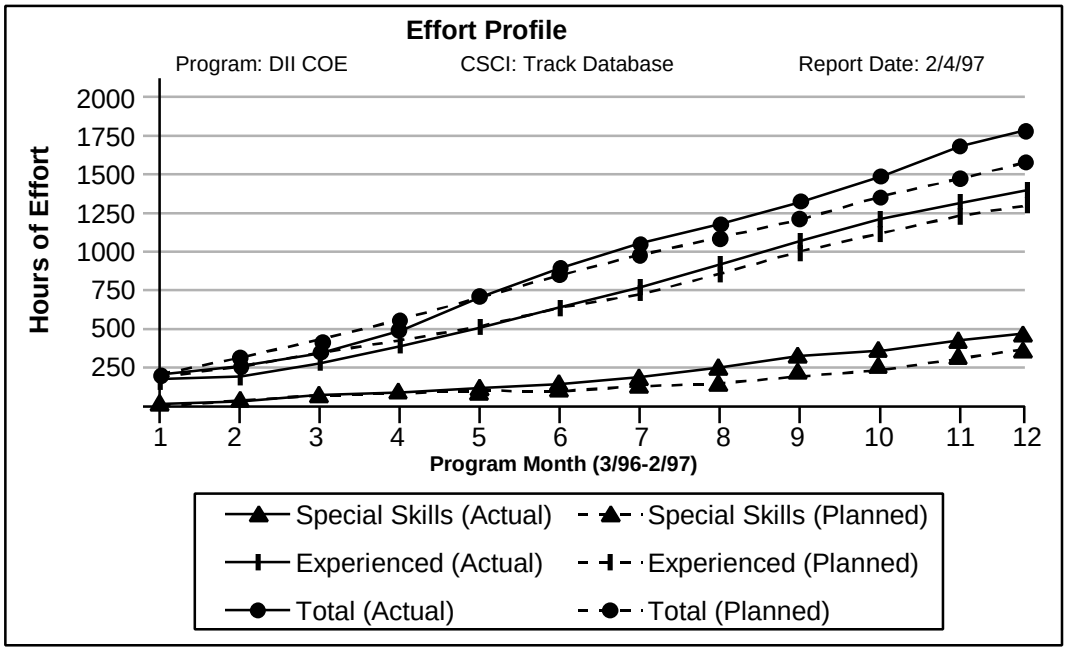

Figure B-5. Sample Graph of Manpower Effort Measure

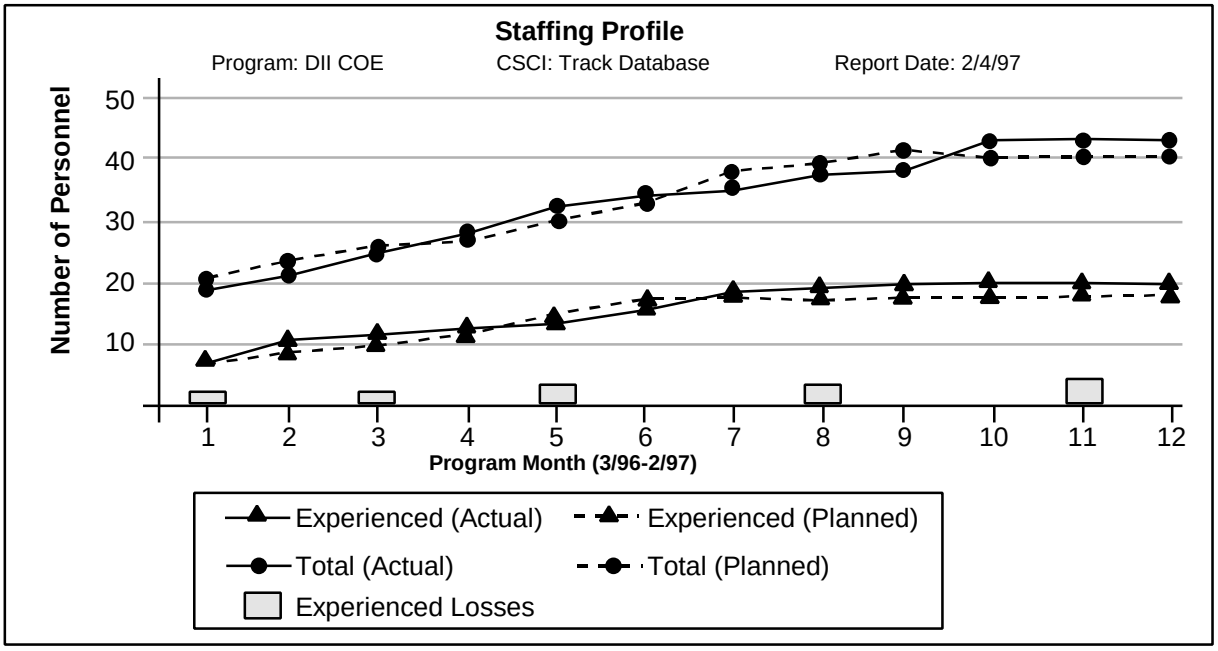

Figure B-6. Sample Graph of Manpower Staffing Profile

The Project Control Panel gauges, described in *The Program Manager's Guide to Software Acquisition Best Practices*, also provide manpower metrics: (1) Voluntary Turnover Per Month [Project Control Panel Gauge #11], and (2) Overtime Per Month [Project Control Panel Gauge #12]. Voluntary Turnover Per Month is calculated by dividing the number of staff leaving during each reporting period by the number of staff at the beginning of the reporting period. The result is to be expressed as a percentage. The target range is less than 2 percent per month. A person can leave the project in a number of ways, such as quitting the organization or requesting reassignment to another project. Turnover is an important measure for risk assessment. Each project member who leaves the team causes a productivity drop and schedule disruption.

Overtime Per Month is calculated by dividing the overtime hours by the base working hours for all project staff in the reporting period. It is expressed as a percentage. The target range is less than 10 percent. When overtime rate approaches 20 percent, the ability of staff to respond effectively to crises suffers significantly.

B.4 COTS License Management Metric

COTS License management measures and compares the acquisition, distribution/allocation and use of COTS licenses by system users. COTS license requirements are estimated by determining the number of segments requiring licenses in a given software build/release and the number of anticipated DII COE products required by customers. Actual data on license procurement, distribution, use, and requests, both fulfilled and unfulfilled, is tracked and compared with initial estimates. The need to adjustment license management strategies may be indicated if estimates fall below or above actual license usage data. In addition, potential opportunities for cost-effective procurement strategies, such as enterprise licensing, can be identified and justified based on analysis of current license usage and trends.

B.5 Requirement Traceability Metric

Requirement traceability measures the level to which software p roducts have implemented requirements allocated from higher level specifications. Software products include specifications, software design, code, and test cases.

The requirements traceability metrics are an accounting of how many requirements from one document are addressed in other documents. In order to do this, the hierarchy of technical documentation must be determined, and the relationship between the requirements in the different documents evaluated. The objective is to be able to trace requirements from top-level operational requirements down to code and test cases and to verify that all higher level requirements are allocated to lower levels and that lower levels do not add any new requirements. The primary measure collected in requirements traceability metrics is the account of requirements successfully traced from one level to another. As a minimum, the percent traceable from the SRS to code and SRS to test cases should be provided. The recommended level of reporting software requirements traceability data is at the CSCI level. For each level of requirements tracing, the following information is collected:

1. Names of two documents assessed.
2. Number of system/software requirements in the “traced from” document.
3. Number of requirements in the “traced from” document successfully traced to the “traced to” document.
4. Number of requirements in the “traced from” document that could not be traced to the “traced to” document.
5. If a backward trace is also performed, record the number of requirements in the “traced to” document that were successfully traced back to the “traced from” document and the number of requirements in the “traced to” document that could not be successfully traced back to the “traced from” document.

Figure B-7 is an example graph recommended for the requirements traceability metric. The chart provides a summary of a CSCI’s software requirements traced forward to lower levels of design and code and backward to system requirements. Similar graphs could be used to identify requirements that address key user operations and critical functions.

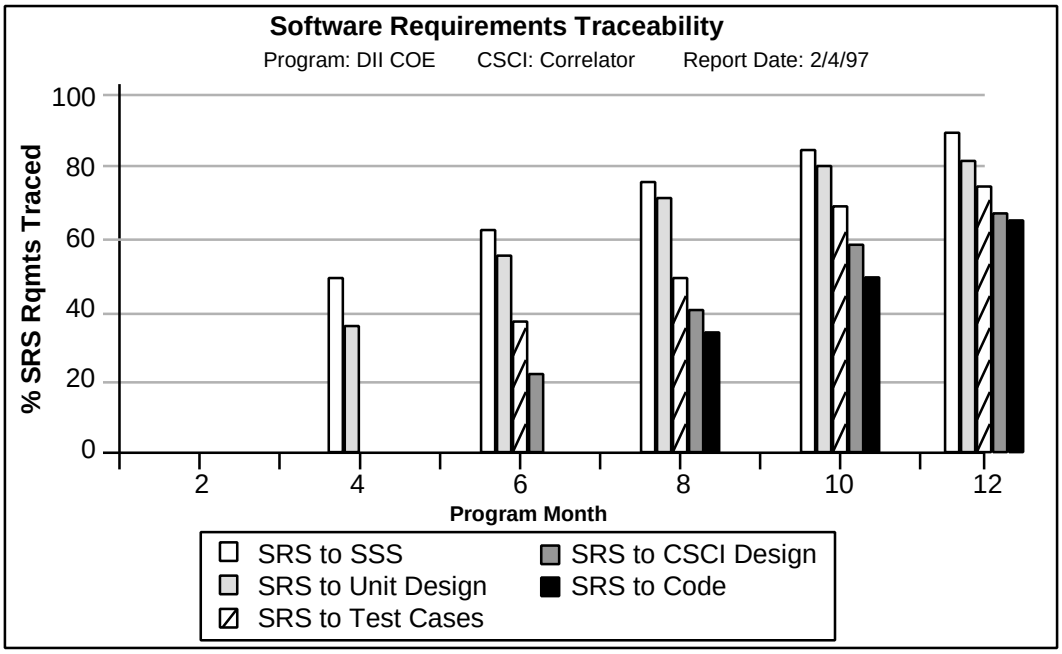

Figure B-7. Sample Requirements Traceability Graph

B.6 New Requirements Metric

The new requirements metric measures the amount of time required for new requirement processing tasks according to requirement priority and level of effort to implement. This measurement encompasses the entire new requirement cycle in terms of the number of calendar days between significant events. Data collected is averaged for the scheduled periods for each new requirement. Captured data may be presented similar to the way ECP cycle data are presented in Paragraph B.8.

B.7 Requirements Change Per Month Metric

The Requirements Change Per Month metric is calculated by dividing the number of new, changed or deleted requirements specified in the current reporting period by the total number of requirements at the end of the current period. It is expressed as a percentage. Typical projects experience a requirements change of 1% per month.

B.8 Change Request/Proposal Metric

The change request/proposal metric measures the amount of time required for ECP processing tasks according to ECP priority and level of effort to implement. This measurement encompasses the entire ECP cycle in terms of the number of calendar days between significant events. Data collected is averaged for the scheduled periods for each ECP. Data are typically presented as (1) a pie chart showing percentage of time spent in portions of the cycle (see Figure B-8) , or (2) bar charts showing portions contributing to lateness (see Figure B-9). This data may be stratified by ECP $ value, complexity factors, or priority codes to determine the influence of such factors on processing time.

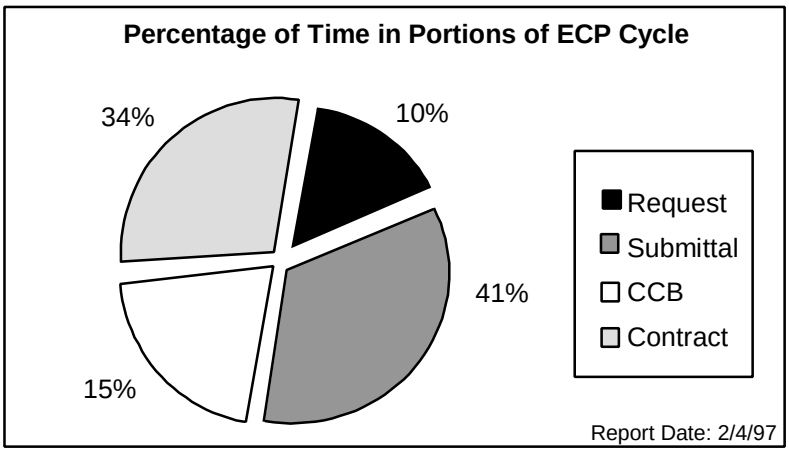

Figure B-8. ECP Cycle Chart

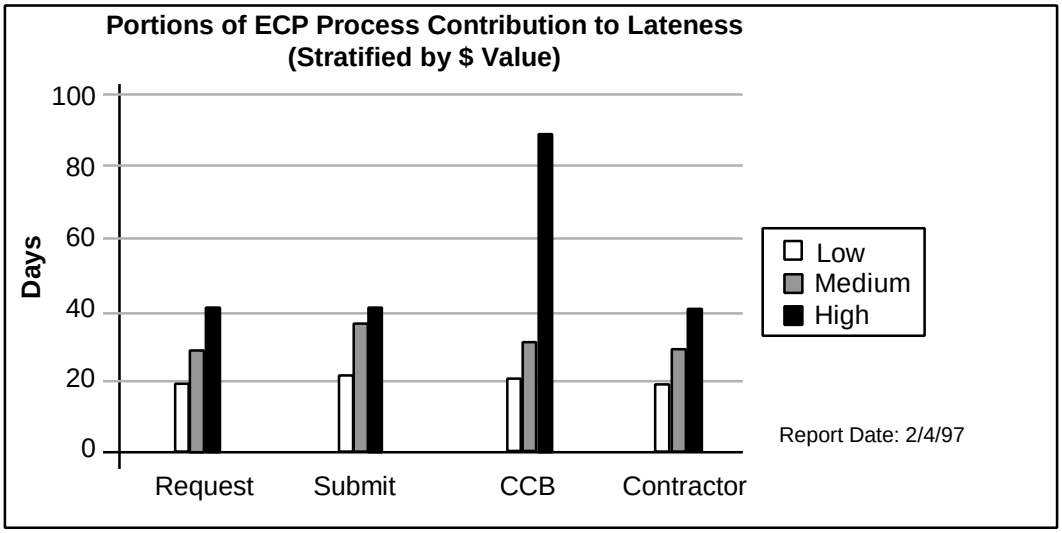

Figure B-9. ECP Process Delays

B.9 ECP Approval Rate Metric

This metric applies only to Class I ECPs. To obtain a measure of the rate of first pass approvals in any time period, count the number of ECPs that are approved upon first submittal to a CCB, and divide by the total number submitted. Do not count the nuber of ECPs that are revised and resubmitted as first pass approvals. Monthly or quarterly compilation is typical, depending upon change volume. A recommended display of ECP approval rate data is shown in Figure B-10.

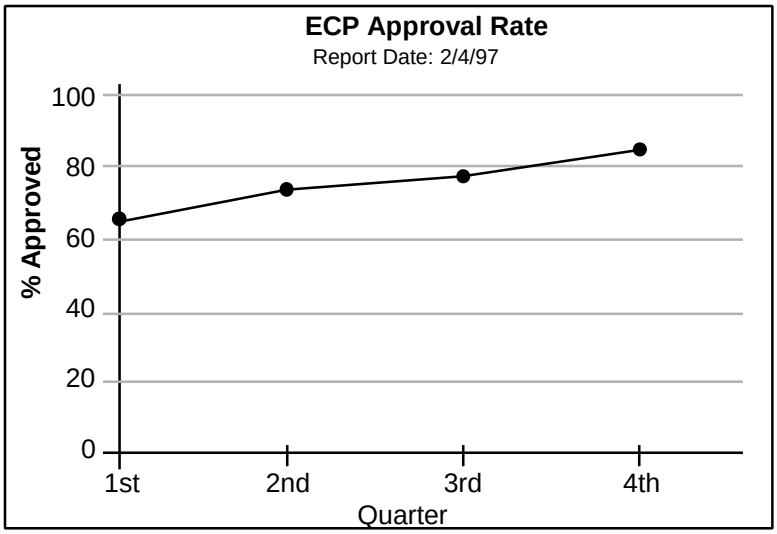

Figure B-10. ECP Approval

B.10 Quality Gate Task Status Metric

The Quality Gate Task Status shows the completion status of tasks during the current reporting period. A *quality gate* is a predefined completion criterion for a task. The criterion must be an objective yes/no indicator that shows a task has been completed. The indicators are:

1. **Total Due** is the total number of tasks scheduled for completion during the current reporting period plus any overdue tasks from previous periods. This indicates the total quantity of work required for the project to keep pace with the schedule.

2. **Completed On Time** is the number of tasks originally scheduled for completion during the current reporting period that were completed by their originally scheduled due date. This number indicates how well a project is keeping up with scheduled work.

3. **Completed Late** is the number of tasks completed late during the current reporting period. This number includes those tasks scheduled for the current period that were completed late, as well as any over due tasks from previous periods that were completed in the current period. The Completed Late number indicates how well the project is completing work, even if it is late according to the original schedule.

4. **Total Overdue** is the total number of tasks for all previous reporting periods that are overdue by the end of the current reporting period. This is an indicator of the quantity of work needed to get the project back on schedule.

B.11 CM Churn Per Month Metric

The CM Churn Per Month metric is calculated by taking the number of baselined CIs that have been modified and rechecked into the CM system over the last reporting period and dividing by the total number of baselined CIs in the system at the end of the period. It is expressed as a percentage. A modified CI is one that was previously in the system, but was reviewed sometime later and then modified or relaced. This gauge serves as an indicator of the architectural soundness of the system. If the rate of churn begins to approach the 2% per month level, this shows a lot of rework is going on and that either the original design was not robust enough or requirements are changing.

B.12 Segment Submissions Metric

The segment submissions metric measures the number of segments submitted manually (successfully vs. unsuccessfully) and the number of segments submitted electronically (successfully vs. unsuccessfully) during a given time period. This data may be stratified by segment size (MB) or contractor. Another measurement for this metric might include the number of segments submitted that were not pre-registered.

B.13 Asset Distribution Metric

The asset distribution metric measures the number of segment requests received and processed (successfully versus unsuccessfully) and the number of times segments were distributed manually versus electronically (successfully versus unsuccessfully) during a given time period. This data may be stratified by segment types or receiving organization.

B.14 Design Stability Metric

The design stability metric is composed of two measures. The design stability measure tracks changes made to the design of the software. The design progress measure shows how the completeness of the design is advancing over time. To determine design stability the following information is collected for each CSCI and each delivery/design version:

1. Date planned for design/delivery version completion.
2. M = Number of units in current delivery/design.
3. F_c = Number of units in current delivery/design that include design related changes from previous delivery.
4. F_a = Number of units in current delivery/design that are additions to previous delivery.
5. F_d = Number of units in previous delivery/design that have been deleted.
6. T = Total number of units projected for system. If tracking design stability for builds or increments, T will reflect the total number of units projected for the build.

From this information the design stability (S) and design progress (DP) can be calculated as follows:

$$S = [M - (F_a + F_c + F_d)] / M$$

$$DP = M / T$$

The design stability measure depicts how much of a software delivery, or version, is comprised of pieces reused without modification from the previous delivery or version. The closer this value is to one, the higher the amount of reuse. Plotting the calculated design stability (S) and design progress (DP) values over time, as shown in Figure B-11, is recommended for data display. The higher the design stability measure, the better the chances of a stable software configuration.

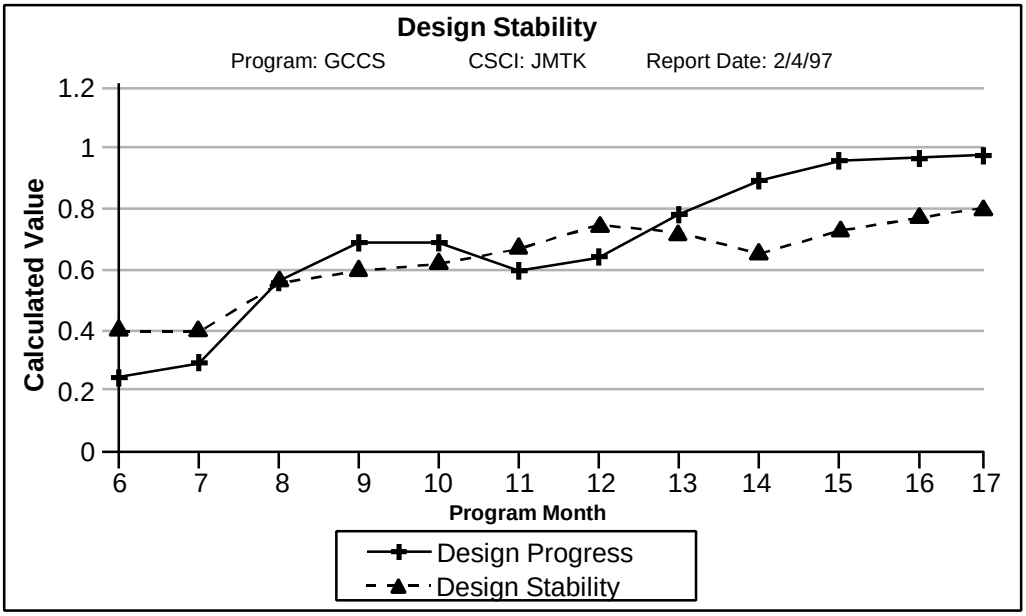

Figure B-11. Sample Design Stability and Design Progress Graph

B.15 Breadth of Testing Metric

Breadth of testing addresses the degree to which required functionality has been successfully demonstrated as well as the amount of testing that has been performed. For the breadth of testing metric the following information is collected for each CSCI, each formal test, and each requirement type:

1. Type of requirements tested and validated (such as SRS, IRS, etc.).
2. Total number of that requirement type allocated to the CSCI.
3. Number of requirements tested with all planned test cases.
4. Number of requirements successfully demonstrated.
5. Test identification (e.g., CSCI (or system) qualification testing, compliance testing, Development Test (DT), Operational Test (OT)).
6. Requirements priority or criticality, if any.
7. Number of SLOC affected by approved ECPs.

The requirement counts collected in the breadth of testing metric can be used to compute three different measures of testing progress as shown by Figure B-12. Each value can be multiplied by 100 to derive a percentage. All three test progress measures can be simultaneously displayed over key test events as shown in Figure B-13. The overall success measure provides insight into the level of progress made toward implementing the approved requirements baseline. When changes are made to requirements or design, previous test results for those areas are no longer valid. The number of requirements tested and number of requirements passed should drop by the number of requirements to be retested.

Measure	Formula	Addresses
Test coverage	(Number of requirements tested) / (Total number of requirements)	How much of the total was tested, without regard to test success.
Test success	(Number of requirements passed) / (Number of requirements tested)	How much of what was tested was successful.
Overall success	(Number of requirements passed) / (Total number of requirements)	How much of the total was tested and successful.

Figure B-12. Testing Progress Measures

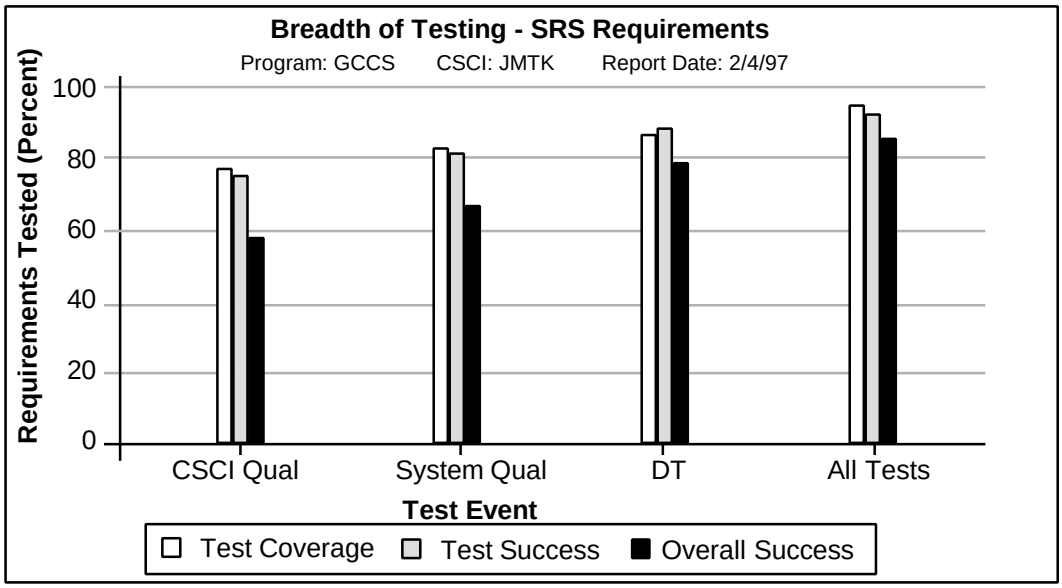

Figure B-13. Sample Testing Process Graph

B.16 System Thresholds Metric

The system thresholds metric summarizes data derived from comparisons of DII COE thresholds with performance parameters observed during various software testing activities, including integration test, compliance test and interoperability testing. Threshold violations are tracked by type (e.g., message processing rate, query response time, queue overflow, database overload, etc.), by the CSCI, or segment, to which the threshold applies, and by the activity/process that detected the threshold violation.

B.17 Fault Profiles Metric

The fault profiles metric provides a summary of software problem/change report (GSPR) data collected by the corrective action system. This metric provides insight into the number and type of deficiencies in the current software baseline, as well as the developer's ability to fix known faults. For the fault profiles metric the following information is collected for each CSCI, each fault priority, and each fault category:

1. Cumulative number of faults detected.
2. Cumulative number of faults closed.
3. Average age of open faults.

4. Average age of closed faults (same as average time to close).
5. Average age of all faults.

Fault counts should be based on all tests and evaluations performed on a formal baseline under configuration control. Average ages can be computed using the formulas in Figure B-14.

Average Age of	Formula
Open faults only	(The sum of the days between the time each open fault was detected and the current date) / (Total number of open faults)
Closed faults only	(Total number of days all closed faults remained open) / (Total number of closed faults)
All faults (open and closed)	(The sum of the days between the time each open fault was detected and the current date, plus the total number of days in which all closed faults remained open) / (Total number of open and closed faults)

Figure B-14. Computing Average of Fault Ages

Inadequate problem resolution by the developer can cause the cumulative number of closed faults to remain constant over time, and a number of faults will remain open. The age of the open faults should be checked to see if they have been open for an unreasonable period of time. Those faults that are not resolved represent an increased risk. Average age graphs can track whether the time to close faults is increasing over time. Increasing time to close faults may indicate that the developer is not allocating adequate resources to correcting problems, or that some faults are exceedingly difficult to fix.

A common display of fault profiles metrics data is shown in Figure B-15 as the cumulative numbers of software faults detected (problem reports opened) and closed, over time. An alternate display of corrective action activity is to plot the number of problem/change reports that were opened and the number closed over periodic intervals, such as months. Figure B-16 is an example of monthly GSPR opening and closure activity for one CSCI. Figure B-17 is a graph of the average length of time a fault not yet resolved has been in the corrective action system.

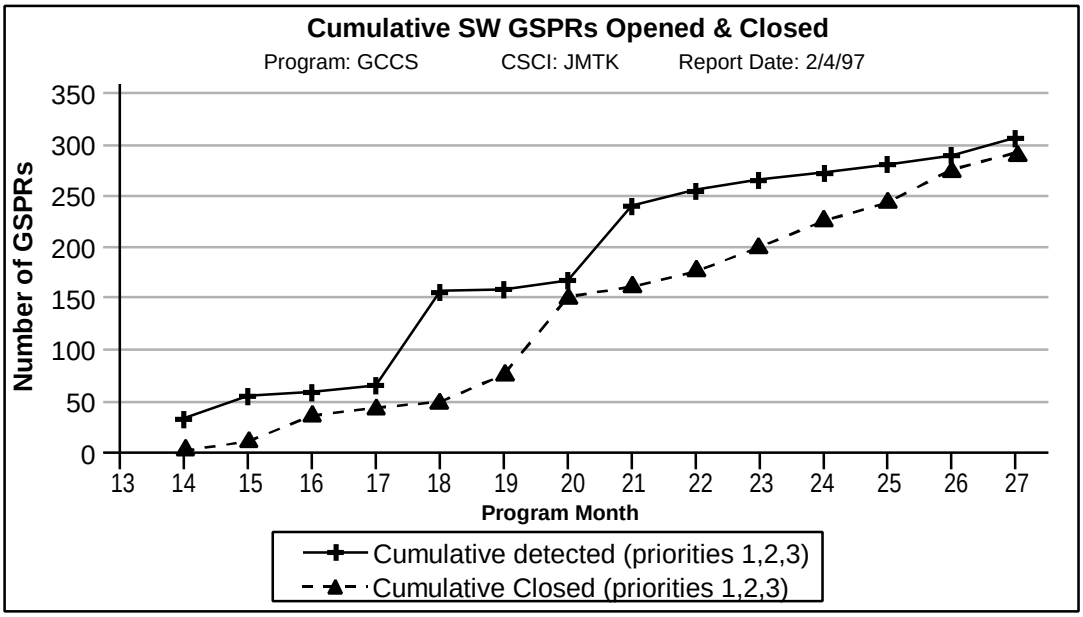

Figure B-15. Sample Graph of Software Problem History

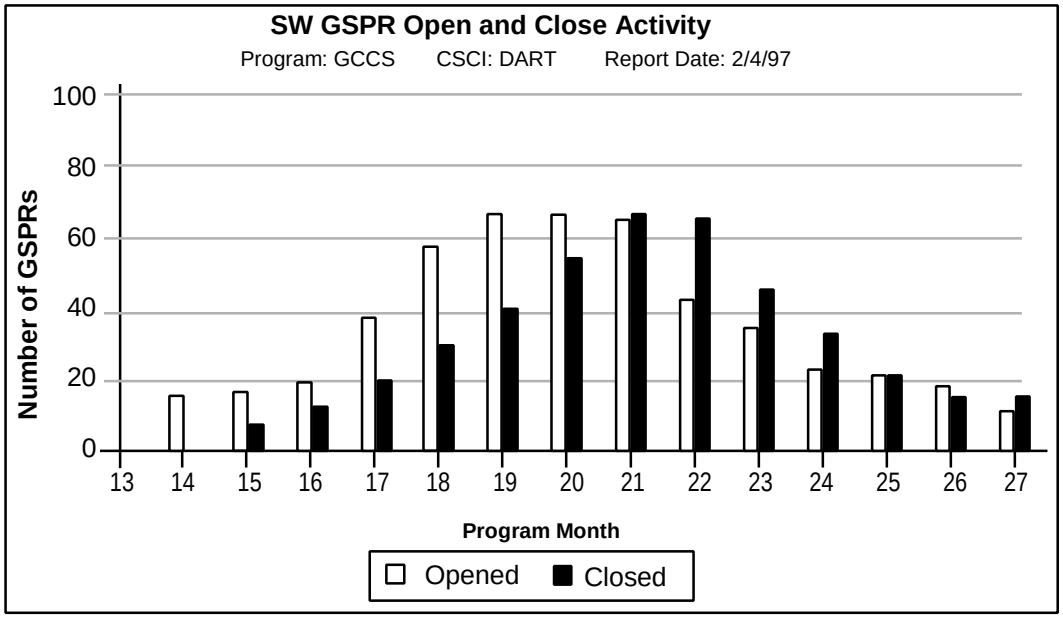

Figure B-16. Example of Monthly GSPR Activity

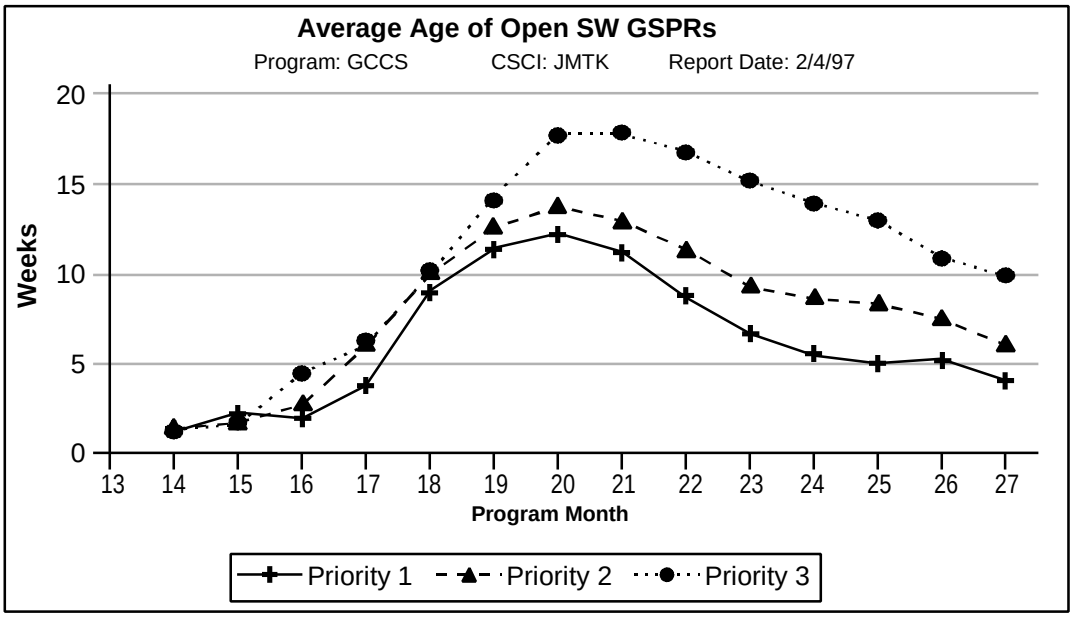

Figure B-17. Sample Graph of Average Age of Open Faults

B.18 Deviation Profiles Metric

The deviation profiles metric provides a summary of deviations requested by developers for software and documentation deliveries. This metric provides insight into how Requests for Deviation are being used and the frequency of their use. For the deviation profiles metric the following information is collected for each Request for Deviation:

1. Requesting Organization/Contractor

2. CSCI(s)/Segments impacted
3. Documentation impacted
4. Whether deviation approved or disapproved
5. Deviation effectivity date and expiration date
6. The number of times the specific deviation has been requested/renewed
7. Classification of the deviation: minor, major, or critical.

Deviation profiles data collected can be plotted over time, by requesting organization/developer, by segment, or by type of deviation to identify potential problem areas and determine if further investigation is required.

End of Document